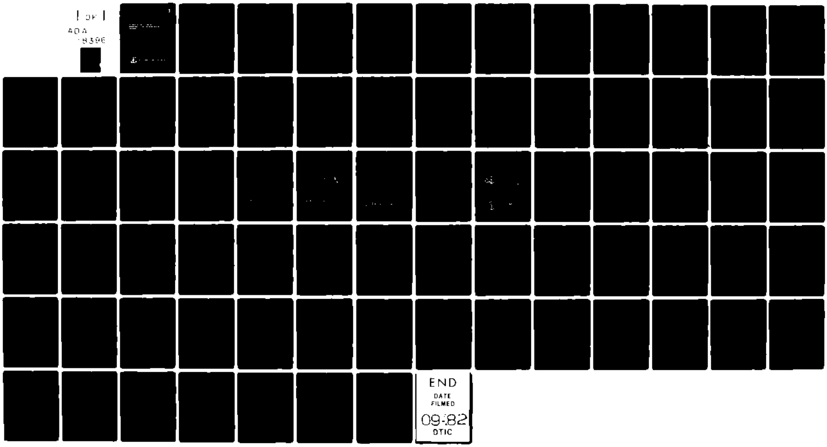
AD-A118 396   NAVAL SURFACE WEAPONS CENTER SILVER SPRING MD   F/G 15/3
PHYSICAL SECURITY MODELING FOR THE SHIPBOARD NUCLEAR WEAPONS SE--ETC(U)
APR 82   E G JACQUES, D L BARTUSEK, R W MONROE
UNCLASSIFIED   NSWC/TR-82-50   SBI-AD-F500 051   NL

1 OF 1
ADA
118396



END
DATE
FILMED
09-82
DTIC

NSWC TR 82-50

PHYSICAL SECURITY MODELING FOR THE SHIPBOARD NUCLEAR WEAPONS SECURITY PROGRAM

BY E. G. JACQUES D. L. BARTUSEK R. W. MONROE M. S. SCHWARTZ

WEAPONS SYSTEMS DEPARTMENT

1 APRIL 1982

Approved for public release, distribution unlimited.

NAVAL SURFACE WEAPONS CENTER

Dahlgren, Virginia 22448 • Silver Spring, Maryland 20910

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
NSWC TR 82-50

2. GOVT ACCESSION NO.
AD-A118396

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
PHYSICAL SECURITY MODELING FOR THE SHIPBOARD NUCLEAR WEAPONS SECURITY PROGRAM

5. TYPE OF REPORT & PERIOD COVERED

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
E. G. Jacques R. W. Monroe
D. L. Bartusek M. S. Schwartz

8. CONTRACT OR GRANT NUMBER(s)

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Naval Surface Weapons Center
White Oak
Silver Spring, Maryland 20910

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
PE 63571 N, S0812SL, S0812L001, N78

11. CONTROLLING OFFICE NAME AND ADDRESS

12. REPORT DATE
April 1982

13. NUMBER OF PAGES
76

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)

15. SECURITY CLASS. (of this report)
UNCLASSIFIED

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Approved for Public Release; Distribution Unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)
Security Model, Scenario Model, Insider Model, Outsider Model

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

A modeling methodology in support of the Shipboard Nuclear Weapons Security program was needed in order to allow a trade-off of various candidate security systems. This document details the factors that lead to the modeling approach currently being used. In addition a brief description of the models along with examples is presented. The models were chosen for their ability to analyze the spectrum of potential threats pertaining to the operational conditions of a variety of ship classes.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

FOREWORD

In 1978, the Shipboard Nuclear Weapon Security (SNWS) Program was initiated at NSWC in order to provide the Navy with improved physical protection of its nuclear weapons. System analysis and system modeling are important functional areas within the SNWS program and organizationally occupy a position between the requirements analysis and technology development tasks on one hand and system concept formulation on the other. Thus the system modeling effort was created to support both the assessment and design functions during the iterative process to obtain the best overall security system from the resources available.

Although individual devices had been modeled before on a piecemeal basis, physical security analysis at a system level was a relatively new field. The first chapter of this report presents a review of the status of security modeling at the time of initiation of this task, including a survey of the models then operable as well as what efforts were currently being pursued by both governmental agencies and private concerns. The criteria for comparing models is discussed in the context of deciding what programs could be adapted for use on the SNWS program as well as the need for initializing new efforts to accommodate any special requirements peculiar to the project. Finally, the three programs comprising the foundation of the SNWS modeling effort, SAFE, SNAP, and MAIT, are presented in three separate chapters with the emphasis on the problem to be solved and how the model solves it. The mechanics of calculation and other such detail have been omitted in favor of focusing on the way the individual program fills a particular SNWS modeling need. However, a bibliography is included with each model that can provide the reader with as much background and mathematical depth as desired.

JOHN M. WACK
By direction

CONTENTS

CHAPTER		PAGE
1	SELECTION OF SYSTEM MODELS FOR THE SNWS PROGRAM	1-1
	INTRODUCTION	1-1
	EXISTING MODELING EFFORTS	1-2
	IN-HOUSE SURVEY	1-2
	GOVERNMENT AND PRIVATE SURVEY	1-3
	INDEPENDENT CONTRACTOR'S SURVEY	1-7
	ASSESSMENT CRITERIA	1-8
	MODELING ENHANCEMENTS TO SUPPORT SNWS	1-10
2	SAFE	2-1
	INTRODUCTION	2-1
	PROBLEM ADDRESSED	2-1
	DESCRIPTION OF THE PROGRAM	2-2
	INTRODUCTION	2-2
	METHODOLOGY	2-2
	FACILITY CHARACTERIZATION	2-2
	FACILITY REPRESENTATION	2-3
	COMPONENT PEFORMANCE SELECTION	2-3
	ADVERSARY PATH ANALYSIS	2-4
	EFFECTIVENESS EVALUATION	2-4
	SNWS IMPLEMENTATION	2-5
	PROGRAM RUN ARCHITECTURE	2-5
	COMPUTATIONAL REQUIREMENTS	2-6
	REFERENCES	2-14
3	SNAP	3-1
	INTRODUCTION	3-1
	PROBLEM ADDRESSED	3-2
	DESCRIPTION OF THE MODELING APPROACH	3-2
	SYMBOLOGY	3-2
	SNAP DESCRIPTION	3-3
	INPUT REQUIREMENTS	3-3
	OUTPUT DESCRIPTION	3-5
	SNAP IMPLEMENTATION	3-5
	REFERENCES	3-12

CHAPTER		PAGE
4	MAIT	4-1
	INTRODUCTION	4-1
	PROBLEM ADDRESSED	4-2
	STATEMENT OF THE PROBLEM	4-2
	BACKGROUND AND NATURE OF SOLUTION	4-3
	DESCRIPTION OF THE PROGRAM	4-4
	INTRODUCTION	4-4
	THE MAIT METHOD	4-5
	ACCEPTANCE CRITERIA	4-5
	DATA COLLECTION AND FACILITY MODELING	4-5
	MAIT COMPUTER ANALYSIS	4-7
	ASSESSMENT	4-8
	MAIT IMPLEMENTATION	4-10
	PROGRAM RUN ARCHITECTURE	4-10
	CURRENT OPERATIONAL STATUS	4-12
	COMPUTATIONAL REQUIREMENTS	4-13
	SAMPLE PROBLEM	4-13
	REFERENCES	4-26

ILLUSTRATIONS

FIGURE	DESCRIPTION	PAGE
2-1	SAMPLE DETERMINISTIC PATHFINDER RUN	2-7
2-2	SAMPLE STOCHASTIC PATHFINDER	2-8
2-3	SAMPLE PATH DISPLAY	2-10
2-4	SAMPLE EASI RUN	2-11
2-5	SAMPLE EASI GRAPHICS	2-12
2-6	SECTIONS OF A SAMPLE DATE RUN AND SUMMARY OF EFFECTIVENESS MEASURES	2-13
3-1	FACILITY NODE DIAGRAM	3-6
3-2	GUARD SUBNETWORK	3-7
3-3	ADVERSARY SUBNETWORK	3-8
3-4	PORTION OF SNAP TRACE	3-9
3-5	SYSTEM PERFORMANCE STATISTICS	3-10
3-6	NODE STATISTICS	3-11
4-1	MAIT METHODOLOGY	4-13
4-2	PROGRAM RUN ARCHITECTURE	4-14
4-3	SAMPLE PROBLEM LAYOUT	4-15
4-4	SAMPLE PROBLEM PARAMETERS	4-16
4-5	SAMPLE PROBLEM INPUT	4-18
4-6	SAMPLE PROBLEM OUTPUT	4-19

TABLES

TABLE		PAGE
1-1	PHYSICAL SECURITY MODELING PROGRAMS - 1979	1-4
1-2	SNWS PROGRAM ORGANIZATION	1-12

CHAPTER 1

SELECTION OF SYSTEM MODELS FOR THE SNWS PROGRAM

INTRODUCTION

The Shipboard Nuclear Weapon Security Program (SNWS) was initiated at NSWC in 1978 in order to provide the Navy with better physical protection of its nuclear weapons. The gravity and permanence of the nuclear security problem has warranted a complete "top-down" long-range program by the Navy as opposed to a quick-fix interim solution. Because this global approach affords a greater degree of freedom in resolving the problem addressed, system analysis and system modeling have inherently become important task areas in the overall program.

Two questions pertaining to the modeling effort became apparent immediately at the onset of the SNWS program: 1) what existing security modeling programs are already available, and 2) what will be needed to satisfy the SNWS effort in particular. A perfect match between these two requirements would have all but eliminated the need for the program to initiate a modeling effort but obviously such an ideal situation did not exist. This incongruity was due to not only the incompleteness of coverage by existing programs but also to the additional requirements imposed by factors peculiar to shipboard environments. After ascertaining from steps 1 and 2 above what areas would remain uncovered if currently available programs were used, it was decided that the best way to fill the entire spectrum of SNWS modeling would entail two additional phases: 1) where possible, modify the existing program to fit the SNWS needs, and 2) initiate ground-start modeling efforts to fill any remaining sectors deemed necessary for the impending analysis.

This 2-directional approach was decided upon for several reasons. Although it would have been aesthetically pleasing to design programs for every facet of the SNWS modeling effort from the ground up, practical time and cost limitations precluded this course of action. A small but capable community of security modelers already had been working in this field for several years and not to capitalize on their experience and expertise where possible would seem a flagrant waste. On the other hand, to try to "shoehorn" the entire SNWS modeling task into then existing programs would have been of equal folly since we would be designing the problem to fit the tools. In summary, it was agreed that the modification plus supplementation approach would result in the best long-range security modeling capability and yet remain within the confines dictated by time and money considerations.

The remainder of this Chapter discusses the situation at the time that the SNWS modeling effort began, the criteria for evaluating security modeling programs, and the basis of selecting particular programs in view of the overall task. It should be emphasized that throughout this report references to such phrases as "modeling effort" and "program" are not intended to restrict attention to the digital computation process alone. Indeed, it is the entire modeling methodology that is of importance in determining its applicability to the SNWS program and the actual computer code may be but a small part of this process. The mechanical crunching of numbers by the computer is of little value unless it is guided by the knowledge and judgment of the individual analyst.

EXISTING MODELING EFFORTS

As discussed above, one of the first tasks facing the system modeling group was determining what applicable programs were then in existance and what effort was currently being expended in both governmental and private sectors. A 3-phase plan was initiated to accomplish this task consisting of: 1) an in-house survey, 2) visitations to possible candidate concerns working in this field to appraise the status of their efforts, and 3) funding of a private contractor to execute an independent survey. Because of their importance in forming the foundation of the SNWS modeling task, these subtasks are discussed more fully below.

IN-HOUSE SURVEY. The SNWS modeling team initiated a survey of existing models which was divided into two separate phases, the first of which was a literature search. This search was accomplished in the usual but thorough manner of electronically interrogating a data bank containing the listings of several libraries including those of NSWC and a composite of DOD. Although numerous reports pertaining to individual protection devices were listed, those describing overall methodologies were almost nonexistent. This was not unexpected since most efforts in the security modeling field in 1979 were fairly new and also much of the information was considered proprietary and did not find its way into library systems. It must be remembered that at this time physical security was approached in a piecemeal fashion and that top-down design was a relatively new concept that was just being initiated for nuclear facilities and a few other industrial applications. In summary, the prime benefit of the library search was in the drawing of attention to governmental agencies and private concerns currently engaged in physical modeling and not in the revelation of applicable individual reports.

Armed with the partial list of participating governmental agencies derived from the library search, the modeling team was now in a position to make direct inquiries into these activities. As is the case of investigating any relatively specialized field of endeavor, once a "toehold" was established within the community, a fanning out through personal contacts and cross-referencing revealed which agencies and private concerns were involved and to what degree. It soon became obvious that the most comprehensive modeling efforts were rooted in the Nuclear Regulatory Commission and Sandia Laboratories although some specialized programs were being conducted by other organizations. A more complete list of the governmental agencies and private concerns that were felt most likely to be doing work relevent to the impending SNWS modeling task was now able to be assembled and this formed the basis of the plant visitations discussed below.

GOVERNMENT AND PRIVATE SURVEY. As suggested above, the community involved in physical security modeling was relatively small in 1979 although the funding through Federal agencies was appreciable and growing. This prompted the SNWS modeling team to arrange visits to those agencies most actively involved as a first step to be followed by visitations to the private contractors themselves.

Among the Federal agencies visited were the Nuclear Regulatory Commission (NRC), the Defense Nuclear Agency (DNA), as well as an additional agency with a classified charter. Also, conversations with the appropriate branches of the Military Services were held to determine the state of their physical security modeling efforts. In summary, it was found that the bulk of the system programming was being funded by NRC either directly to the private contractors or through Sandia Laboratories which, aside from monitoring these contracted efforts, were themselves doing extensive research into this area. However, some of the other efforts, although more concentrated in scope, were equally viable as candidates for the SNWS program.

The list of private contractors to be visited by members of the SNWS modeling team included Sandia Laboratories, Science Applications, Inc. (SAI), Lawrence Livermore Laboratories (LLL), Mission Research Corp. (MRC), and TRW. Although Table 1-1 summarizes some of the particulars of each of these efforts, a few additional observations relevent to early 1979 should be made. Sandia had not only been in security evaluation the longest, but had by far the largest ongoing effort at that time. This was embodied in a myriad of programs which reflected a wide range of capabilities including automatic digitization of blueprints for facility representation, numerous optimal pathfinding techniques, barrier evaluation, small combatant modeling, and entire security system evaluation. Although most of these models were designed for a singular purpose, the importance of tying them together to produce a homogeneous assessment of the entire security system had not escaped Sandia's thinking. Indeed, most of their effort by 1979 was directed at this goal as opposed to designing new individual pieces notwithstanding that updating and refinement were a continual process. The SAFE program, one of those ultimately chosen for the SNWS program, is really a set of individual subprograms combined in a manner to produce a unified result. Finally, it should be noted that most of Sandia's programs were actually developed, up and running, and in varying states of verification as opposed to something merely in the "would like to do" stage, a malady we often found with respect to physical security programs.

TABLE 1-1 PHYSICAL SECURITY MODELING PROGRAMS - 1979

Sandia Laboratories; Albuquerque, NM

SAFE	Safeguards Automated Facility Evaluation
ISEM	Insider Safeguards Effectiveness Model
FESEM	Forcible Entry Safeguards Effectiveness Model
FSNM	Fixed Site Neutralization Model

Science Applications, Inc.; La Jolla, CA

MAIT	Matrix Analysis of the Insider Threat

Pritsker and Associates; West Layfayette, IN (for Sandia)

SNAP	Safeguards Network Analysis Procedure

TRW; Redondo Beach, CA

SSEM	Site Security Evaluation Model

Mission Research Corp.; Santa Barbara, CA

PSSPAM	Physical Security System Performance Assessment Model

Lawrence Livermore Laboratory; Livermore, CA

SAA	Structured Assessment Analysis
ASM	Aggregated System Model

As can be seen on Table 1-1, SAI currently had two programs under development, MAIT and VISA. MAIT, another program ultimately chosen for SNWS, was unique in that it addressed the insider threat specifically with special consideration of the access and/or control capabilities over safeguards by ship's personnel. VISA, a more ambitious program, was designed to look at both overt and covert threats along various scenario segments including entry, acquisition, and removal and exit or destruction depending whether the mission was theft or sabotage. Although a large sum had been spent, the program was in the state of suspended development and, at the time of this writing, work had not been resumed. For future consideration, the design of the program still appears to be quite valid although considerable work would have to be expended in updating the details in regards to the safeguards themselves.

Lawrence Livermore Laboratories also was engaged in security modeling and had under development a program for assessing material control and accounting systems at nuclear facilities. Their SAA program was structured to produce four levels of evaluation with each stage being successively more stringent. As in the case of the SAI effort, LLL's emphasis was on the insider problem and provided no physical confrontation. An interesting feature was the Boolean representation used to model not only the physical layout but other features such as operational procedures, accountability, and safeguards. This mechanization facilitates use of a common data base for specific scenarios as well as the generation and ranking of critical paths. The first three stages determine respectively if an adversary could reach the target undetected for any path, the probability of detection for the most vulnerable paths, and the effect of random equipment failures. The fourth and most critical level of analysis assumes collusion resulting in the tampering with one or more of the safeguards. At the time of the survey in 1979, the SAA model was still being refined and much work on the last stage in particular remained to be done. The data base to support such a sophisticated program was also an inhibiting factor in consideration for the SNWS task. However, as with SAI's VISA program, the development and use of the SAA program merits monitoring if NSWC continues its physical security efforts beyond the next few years.

LLL also was involved in a figure-of-merit type program called ASM. The purpose of this program was to assess the entire performance of a facility in terms of several measureable criteria including threat, cost, and probability of system win. Although recognizing the need to quantitize these parameters to evaluate system tradeoffs, the immediate applicability of this concept to the SNWS effort seemed nebulous and the risk of time and money in this unproven direction outweighed its potential advantages.

Perhaps the most ambitious model encountered was PSSPAM being developed by MRC. This was an extremely detailed event-based scenario program applicable to the insider and outsider problems with great emphasis on both the physical and psychological composition of the adversaries and guards. A schedule of objectives is assigned for each person which may be reordered, substituted for, or even abandoned depending upon the interaction between the two opposing forces. Much attention is focused on human behavior in specific situations so that not only is the description of the physical locale important but other factors such as tools, weapons, attitudes, skills, and perception (real or envisioned) are equally applicable. Many of the decisional processes were mechanized stochastically necessitating a Monte Carlo execution if meaningful results were to be obtained. Although three levels of detail were to be provided for, only a skeletal outline embodying the lowest level of detail was available at the time of the visit. Our original assessment that PSSPAM, with its voluminous but then unavailable data requirements, would be too late for the SNWS project was eventually proven accurate when development of the program was terminated in 1981. The concept and objectives of PSSPAM still remain valid however, and revitalization of the program in abbreviated form should remain an optional alternative in the future.

It should be mentioned that MRC, partly in support of the PSSPAM program but also as an independent effort, was evaluating the effectiveness of actual security personnel from a human behavior standpoint. At that time, an MRC experimental psychologist was gathering data from guard forces stationed at various nuclear installations by direct personal interview and by questionnaires. Because of their demonstrated capability in this area, the Naval Personnel Research and Development Center has since contracted with MRC to develop a human behavior model.

TRW was one of the original entrants in the physical protection modeling arena and had developed by 1974 a sophisticated scenario program called SSEM. This is essentially a detection model and does not analyze the confrontation between guards and intruders; (i.e., the guard activity affects detection probability only). SSEM maps the physical representation of the facility including barriers, guards, alarms, locks, and other such safeguards into a 3-dimensional orthogonal grid network. Associated with each safeguard is a probability vs. time curve. Thus by using fairly complex numerical analysis techniques involving linear programming, the optimal adversary paths in terms of the lowest probability of detection can be generated and analyzed. Equally important, given a fixed amount of time, the program can compute which paths lie within this limit and yet maintain the least probability of detection. Unlike many of the models already discussed, SSEM was operational and had been applied to several facilities. The main drawbacks to the program, aside from its substantial computer storage and computational time requirements, was the enormous amount of data required to produce the Pd versus time curves for every single safeguard. The required data for all combinations of adversary training, equipment number, skill, experience, etc., as well as details of the safeguard (i. e., thickness of the barrier, material, proximity to guards, etc.) was often subjective at best and in many cases totally unavailable. Although other programs were eventually chosen to perform the outsider scenario analysis, the SSEM approach could still be of value , particularly for predetermined critical paths, provided the data could be obtained and validated.

In summary, the plant visitations were very productive in that they provided a quick but thorough assessment of the current state of physical security modeling. The information gleaned from direct conversation pertaining to such matters as, "who is doing what", "what programs were considered good from a practical point of view as contrasted to theoretical exercises", and "who would like to do what if they had the money", was in many instances as germane to the SNWS program as were the more formal presentations.

INDEPENDENT CONTRACTOR'S SURVEY. Because time was of the essence at this point in the project and also to prevent any omission of consideration of an active modeling effort, it was decided to let a contract with R and D, Associates (RDA) of Arlington, Virginia, to conduct an independent survey "on the availability and capability of computer-based techniques applicable to the modeling of shipboard nuclear weapon physical security systems". RDA was an obvious choice for this contract since they had done a similar survey for the Nuclear Regulatory Commission in 1976-1977 (ref.4-8). The results of their survey, discussed in some detail below, are documented in a report released in October, 1979 (ref.4-5).

To avoid being repetitious, only the highlights of the RDA survey will be presented here although anyone interested in the history of security modeling per se would benefit from reading the entire report. It should be noted that by the time that even a preliminary assessment had been completed by RDA, many of the basic SNWS modeling decisions were in the formulation stage. However, this did not diminish the value of the survey in that it helped ensure that no omissions were made and also as providing for an impartial jury of knowledgeable personnel on which preliminary programming concepts could be tested in the interim.

RDA included all the programs discussed in the section above. Three additional sources of security modeling were listed including Brookhaven National Laboratory, the Air Command and Staff College, and the University of Wisconsin at Oskosh. From the survey's description, these efforts appeared to be inappropriate for the SNWS program due to the fact that they were either in a very preliminary stage of development or that they addressed a problem that was not of direct interest for our mission or that other programs under consideration did the job better. Subsequent direct investigation into these programs verified this conclusion.

The RDA report contains brief descriptions of all the models that were being developed or even in a definitive planning stage. A discussion of each of those efforts is then presented complete with numerous matrices that cross-reference each model against various attribute parameters. These matrices not only helped in the evaluation of the individual programs but also facilitated comparison between them. The report is concluded with some observations about physical modeling in general, complete with bibliography and glossary.

Within the individual model descriptions, RDA included an assessment section where they evaluate the appropriateness of the model in view of the SNWS mission. Although they did not examine the actual computer code to the degree that NSWC did, their coverage of all available documentation was thorough enough to warrant taking their opinions under consideration. RDA seemed to prefer SAFE, MAIT, SNAP, and SSEM for the job categories to which they were assigned, however some reservations were attached to every model. This almost paralleled the preliminary decisions that the NSWC team had already made. Concurrence is not as surprising as it may seem since RDA's main criticisms of individual programs were similar to those of the SNWS team and included: 1) program not operable; program in either a planning or development stage, 2) data is too voluminous or not available at all; data cannot be verified, 3) correct operation of the program requires a level of skill or experience on the part of the analyst that even the developer cannot meet, and 4) excessive run times.

Some summary observations on the general state of security modeling were made by RDA. Perhaps the most interesting of these was the advancement made in the period of 1976 to 1979 when the two surveys were made. RDA cites the increase in range covered, the realism of the programs, and the availability of documentation. Finally, RDA also acknowledged the fact that each model was designed as a separate entity and that the luxury of standard data bases and other such commonality factors is something yet to be achieved. More important, use of independent discrete programs invites voids in the overall analysis which must be recognized and corrected.

In summary, although the results of the RDA survey were not available until many of the preliminary decisions of the SNWS modeling effort were made, the task was still considered of value. Not only did we help ensure that all efforts were investigated, but their observations and criticisms of the individual programs helped shape our thinking pertaining to modifications that would be required in existing programs as well as what new efforts should be initiated.

ASSESSMENT CRITERIA

Since no two physical security models are identical in either purpose or function, some basis of comparison must be established if the selection process is to be a valid one. This section lists some of the parameters associated with security modeling and includes some of the considerations applicable for each parameter. This information is presented in as brief a form as possible in order to keep the verbiage down. These parameters do not cover the entire spectrum of areas of interest associated with each of the programs and, converselу, they are not intended to be mutually exclusive. The purpose of this listing is twofold: 1) to acquaint the reader with some of the considerations and tradeoffs in security modeling, and 2) to present the framework of evaluation from which the SNWS program selection was finally made. The parameters are as follows:

(1) Purpose of program.

What specific problem does the program address; is the program to be used for design or analysis; is the mission sabotage, theft, blackmail, coercion, or something else; does the threat consist of insiders or outsiders or both; what combinations of deceit, collusion, and force are available to the adversaries.

(2) Scope of program.

Where in the spectrum between detailed analysis of a single safeguard at one extreme and the global evaluation of the entire facility at the other does the program reside; does the program operate in a stand alone mode or must it be used in conjunction with other programs.

(3) Program components.

What elements constitute the program such as facility representation, safeguard identification, target designation, path generation, communication, combat engagement, etc.

(4) Mode of operation.

Does the program operate basically in a scenario mode with either time or event or combination thereof used as the independent variable; does the program operate upon the equivalent of a state vector without the use of an independent variable; is the program interactive with the analyst; if so, does the program run in real time; is there any degree of spontaneity required on the part of the analyst; is the program essentially deterministic or is it stochastic in nature; do the calculations rely on mean values or is there a Monte Carlo of random draws.

(5) Pathfinding.

Are all possible paths generated; are paths optimized according to time or probability of detection; of the paths generated, are only a certain amount analyzed based upon some criticality level; can multiple targets be handled; in theft scenarios, are the entrance and exit paths analyzed as one continuous path or as two separate paths.

(6) Data requirements.

How voluminous is the data; is the data readily available or will much time and money have to be spent in obtaining it; can the data be verified; does the data lend itself to incorporation into a common data base that can be used with other programs.

(7) Computational requirements.

How much computer memory core and disk capacity is needed; what peripheral equipment such as tape drives and plotters is needed; how much time does it take to compute a typical case; in what language is the program coded.

(8) Program usability factors.

Is there a long learning curve for the analyst; does the analyst have to understand the internal workings of the program to fully utilize it; what documentation is available; is a user training course provided; program compatibility with other models.

Notwithstanding the fact that all the above criteria did not apply to a single program under consideration, nor could all the attributes of any program be fully described in terms of these parameters, they nevertheless served to form a basis for comparison. The actual classification of requirements needed for the SNWS mission and the way each of these categories was filled is discussed in the following section.

MODELING ENHANCEMENTS TO SUPPORT SNWS

As mentioned above, the basic physical security philosophy for SNWS was to examinine the problem, see what programs were currently available and could be made applicable, and initiate new efforts to fill any voids. Before any decisions pertaining to the selection of individual programs could be made, it became necessary to fully understand how the modeling task was to fit into the entire SNWS program. Table 1-2 depicts the work breakdown of the SNWS program. Functionally, REQUIREMENTS ANALYSIS is the initiating force for all the functional blocks and SYSTEM MODELING lies between TECHNOLOGY ASSESSMENT and DEVELOPMENT OF TECHNOLOGY AREAS and SYSTEM CONCEPT FORMULATION AND ASSESSMENT. The underlying requirement for the system modeling task is embodied in the SNWS Threat Report generated by the Requirements Analysis task. Thus, the modeling block assumes a design as well as an assessment mission. By operating as a buffer between the technology development and the system concept formulation functions, the modeling effort would share both input and output with these groups. Indeed, although shown as three separate functional blocks, tasks would become almost inseparable when viewed from a operational standpoint.

Based upon the overall SNWS mission and the subordinated tasks assigned to the modeling group, the following physical security modeling objectives were established:

Primary requirements:

(a) A global evaluation of entire facility performance.

(b) An outsider scenario model that would include physical facility and safeguard representation, pathfinding, and intervention.

(c) A detailed dynamic response model to analyze the interaction between adversaries and guard forces.

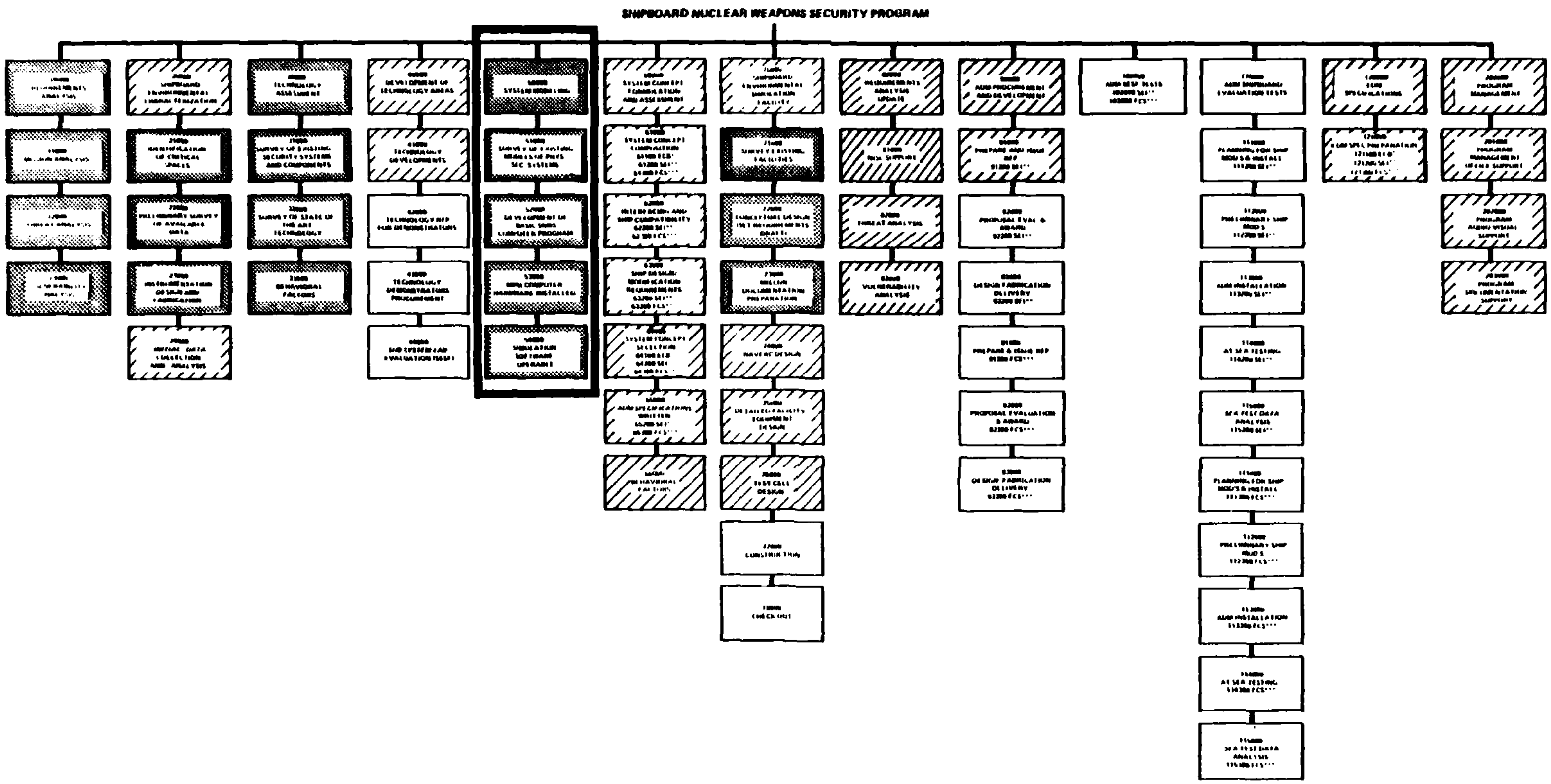
(d) An insider model that considers their unique attributes including stealth, deceit, or abuse of their authorization.

Secondary requirements:

(e) A human behavior model.

(f) A safeguard device model.

TABLE 1-2 SNWS PROGRAM ORGANIZATION


SHIPBOARD NUCLEAR WEAPONS SECURITY PROGRAM
TECHNOLOGY ASSESSMENT
SURVEY OF EXISTING SECURITY SYSTEMS AND COMPONENTS
SURVEY OF STATE OF THE ART TECHNOLOGY
BEHAVIORAL FACTORS
IDENTIFICATION OF CRITICAL AREAS
PRELIMINARY SURVEY OF AVAILABLE DATA
INTERIM DATA COLLECTION AND ANALYSIS
DEVELOPMENT OF TECHNOLOGY AREAS
TECHNOLOGY DEVELOPMENTS
TECHNOLOGY RFP FOR DEMONSTRATIONS
TECHNOLOGY DEMONSTRATIONS PROCUREMENT
SUB SYSTEM LAB EVALUATION TESTS
SYSTEM MODELING
SURVEY OF EXISTING NUCLEAR PHYS SEC SYSTEMS
DEVELOPMENT OF BASIC SNWS COMPUTER PROGRAM
MINI COMPUTER HARDWARE INSTALLED
SIMULATION SOFTWARE UPGRADE
SYSTEM CONCEPT FORMULATION AND ASSESSMENT
SYSTEM CONCEPT COMPOSITION
INTERFACING AND SHIP COMPATIBILITY
SHIP DESIGN MODIFICATION REQUIREMENTS
SYSTEM CONCEPT SELECTION
ADM SPECIFICATIONS WRITTEN
BEHAVIORAL FACTORS
SHIPBOARD ENVIRONMENTAL SIMULATION FACILITY
SURVEY EXISTING FACILITIES
CONCEPTUAL DESIGN
MILCON DOCUMENTATION PREPARATION
NAVFAC DESIGN
DETAILED FACILITY EQUIPMENT DESIGN
TEST CELL DESIGN
CONSTRUCTION
CHECK OUT
REQUIREMENTS ANALYSIS UPDATE
RISK SUPPORT
THREAT ANALYSIS
VULNERABILITY ANALYSIS
ADM PROCUREMENT AND DEVELOPMENT
PREPARE AND ISSUE RFP
PROPOSAL EVAL & AWARD
DESIGN FABRICATION DELIVERY
PREPARE & ISSUE RFP
PROPOSAL EVALUATION & AWARD
DESIGN FABRICATION DELIVERY
ADM DT TESTS
ADM SHIPBOARD EVALUATION TESTS
PLANNING FOR SHIP MODS & INSTALL
PRELIMINARY SHIP MODS
ADM INSTALLATION
AT SEA TESTING
SEA TEST DATA ANALYSIS
PLANNING FOR SHIP MOD'S & INSTALL
PRELIMINARY SHIP MODS
ADM INSTALLATION
AT SEA TESTING
SEA TEST DATA ANALYSIS
SPECIFICATIONS
PROGRAM MANAGEMENT
PROGRAM AUDIO VISUAL SUPPORT
PROGRAM DOCUMENTATION SUPPORT

]

It was felt that if the four primary requirements could be met, the design and analysis tasks could be accomplished. The outsider scenario model is probably the most basic of all the requirements in that it implicitly requires all the fundamental elements such as physical representation, targeting, etc. as noted above. The dynamic response model would afford a more detailed look at the interplay between guards and adversaries as framed in the actual physical representation of the immediate surroundings aboard the ship. Due to the unique features of shipboard environments such as numerous personnel and small, compartmented physical layouts, a model that was particularly addressed to the attributes of the insider and how he could compromise safeguards without resorting to the use of force was considered a necessity. Lastly, the ability to interpret the effect of detailed changes on the entire security system and, in some instances, to be able to compare entirely different approaches to physical security was likewise felt necessary.

The two secondary requirements would have helped fill the voids in the modeling spectrum discussed previously but their usefulness and availability relegated them to a subordinate position. Several of the primary requirements necessitate human reaction and decision modeling at least at a rudimentary level. At the time that our modeling decisions had to be made, there was little evidence that anything beyond assigning a response based upon general scenario characteristics such as immediate physical surroundings, numbers of people involved, training, etc. was still in the experimental stage and could not be substantiated. It may be noted that Sandia in particular attempted to have a human performance model implemented without success (ref.3-6). Thus it was decided to stay with scenario-based probability information rather than try to incorporate detailed behavioral traits that rested on unproven ground. In a similar manner, the device model was also given secondary consideration. As with human performance, more valid data can be obtained by testing the device under actual operating conditions. Each of the primary requirements necessitate describing the safeguards at a level consistent with the overall program. When some preliminary decisions as to what hardware will be included in the system, then the device portion of the modeling effort can be enhanced to perform detailed operational and tradeoff studies.

The final selection process, once framed in the context of the program requirements, was straightforward. First and foremost, the SAFE program of Sandia filled most of both the global evaluation and the outsider scenario requirements. SAFE, as mentioned before, is really a collection of programs that had evolved over several years and which had been expanded to perform numerous individual tasks in physical security assessment. This provided the capability of evaluating a wide latitude of situations ranging from a single path scenario up to a figure-of-merit assessment for the entire facility. Also many unique features had been added that facilitate the analysis which are not identifiable with any single requirement. As an example, an automatic digitizing process that can transform ship blueprints into a mapping directly readable by the computer greatly reduces the laborous task of facility representation. Likewise, a complete 3-dimensional graphics package that plots some given criteria as a function of various safeguard parameters is included. Thus SAFE not only offered SNWS a currently operational tool for global and outsider evaluation, it also represented the results of a long and involved effort by Sandia in the physical security modeling field.

SNAP by Pritsker and Associates (for Sandia) was chosen for the dynamic response model to be used for detailed analysis of small combatant situations. SNAP is an extremely flexible program that is capable of almost any degree of depth that the analyst wishes to pursue. Because of this, the experience and skill of the analyst is paramount in its use. However, since the time span of the SNWS program will be great enough to allow the analyst to come up to speed, it was decided to choose a simulation that could make full use of the analyst's capabilities in the long run.

Most simulation efforts, by both governmental agencies and private concerns, address the safeguard problem as a physical confrontation. This includes variations of both guards versus adversaries and adversaries versus hardware (barriers, locks, alarms, etc,). The approach used most often in these simulations is that an adversary is moved along some chosen path either covertly or overtly encountering safeguards of both types mentioned above along the route. The path is usually determined by some maximizing criteria such as smallest time to target, least probability of detection (Pd), or some combination thereof. If the confrontation is between adversary and device, a mathematical model is used to predict the outcome which may be expressed in Pd or time to defeat. Likewise, if the confrontation is between adversary and guard, a small combat model which considers location and number of each force, weaponry, skill and training, etc. is used to obtain the result. By mathematically combining the predicted outcome of each confrontation, an overall win-lose determination can be made for the entire path. Most models usually have time as the independent variable but some of the more sophisticated approaches use a time-event basis. Lastly, one should note that the models which rely upon probability distributions for estimating results usually can be run in a Monte Carlo fashion to determine some figure-of-merit for the entire safeguard system. But this methodology does not address many of the covert aspects of the insider problem.

To analyze the insider problem, MAIT by SAI was chosen. MAIT is one of the few programs designed exclusively for the insider threat and relies solely on the attributes of authorized access and/or control over safeguards. MAIT represented an approach that was farthest divorced from those used for outsider analysis and it was thought that this diversity would best benefit the overall SNWS effort. Another unique feature of MAIT is that it uses a "state vector" approach and is not time or event dependent.

The apparent voids in the requirements coverage reside in the human behavior and device modeling sectors. As mentioned before, several firms were looking into these areas but proven operational simulations that dealt with these problems specifically were not available then and still are not at the time of this writing. Also, the selected programs cover these topics when needed to the degree consistent with the rest of the coding. It may prove worthwhile to examine the outcome of the current efforts before any new programs are initiated by SNWS.

The remainder of this report describe SAFE, SNAP, and MAIT in the following chapters. The focus of the description is on the problem to be solved and how the program goes about doing this as opposed to the internal mechanics of computation. Also included are the modifications designated by SNWS to make the programs more useful to our particular problem.

Should the reader want more in-depth analysis, bibliographies are provided at the end of each chapter.

CHAPTER 2

SAFE

INTRODUCTION

The Safeguards Adversary Facility Evaluation (SAFE) is a collection of models for physical security system evaluation combined into a continuous sequence of programs. Work on the submodels within SAFE began at Sandia Laboratories in 1974 and after modifications, they were combined to its current format in 1978. Installation on the SNWS Interdata computer began in Jan. 1980. SAFE is currently being used to evaluate physical security for the Navy's ships.

The models included in SAFE are the deterministic critical path analysis model (MINDPT), the stochastic critical path analysis model (PATHS), the adversary interruption model (EASI), and the analytic engagement model (BATLE). The last two, EASI and BATLE, can be run independently as stand-alone programs.

The models, incorporated together into SAFE, perform a global evaluation of a physical security system. Adversary scenarios are generated by selecting optimal paths through the facility for the adversary. The model is analytical in nature and designed to find scenarios meeting specified criteria in a relatively short time.

The emphasis, in SAFE, is on the characteristics of the facility, although a more detailed look at actual scenarios is done when EASI and BATLE are run. In addition, the scenarios selected by SAFE can be input to SNAP for analysis in a scenario-oriented manner.

PROBLEM ADDRESSED

SAFE is used to identify where a physical security system is vulnerable to overt adversary attack. The system is tested for its ability to prevent access to, acquisition of, or removal of protected assets. It looks at the physical characteristics of the facility layout and security system and generates adversary scenarios by finding optimal adversary paths. These paths are selected as optimum based on measures of minimum time, minimum probability of detection, or minimum probability of interruption (timely detection).

A probability of adversary success indicates how vulnerable the system is to attack. When vulnerabilities are identified, changes can be made to the facility representation and to the criteria for selecting optimal paths to further test the system. The scenarios generated can also be looked at in more depth and engagements can be simulated for more specific information.

Since SAFE deals primarily with the physical characteristics of the facility layout and security system, it is best suited for simulating outsider attacks.

DESCRIPTION OF THE PROGRAM

SAFE is actually a collection of programs and supporting utilities which collectively automate the process of analyzing a physical security system.

INTRODUCTION. The SAFE process is made up of five sequential phases. Some are performed entirely by the user and others are automated but require user intervention. The first phase is facility characterization which involves identifying the significant components of the facility. This phase is performed entirely by the user and does not involve use of the computer. The second phase is facility representation which involves converting a description of a facility into an equivalent computer representation. This phase is performed by the user with the help of a Tektronix 4050 Series desk-top microcomputer and a Talos digitizer. The third phase is component performance selection which involves describing the characteristics of the significant components of the facility. This phase is performed by the user with the help of an automated program run on the main computer. The fourth phase is adversary path analysis which involves generating critical adversary paths and analyzing them. This phase is performed by an automated procedure running on the main computer which requests input from the user. The fifth phase is effectiveness evaluation which involves evaluating the security system for its effectiveness against adversary attack and analyzing scenarios in further detail. This phase is also performed by the computer. Each one of these will be explained in further detail.

METHODOLOGY. The SAFE methodology can be broken into several manual and data processing steps necessary for the complete analysis of a security system.

Facility Characterization. During this phase the following facility characteristics are determined:

(1) The facility layout characteristics.

(2) The targets and vital areas.

(3) The operational conditions.

(4) The environmental conditions that are relevant to the specific site.

(5) The components of the physical protection system and their location.

(6) The characteristics of the security forces.

(7) The threat characteristics.

The information needed for performing such an analysis on a ship may be obtained from ship plans. The set of components selected should include only those which contribute to the evaluation of the security system. More detail can be added later if it is needed.

Upon completion of this phase the user should have a list of barriers, penetration points, targets and stairwells. The barriers are the obstacles to adversary movement and the penetration points are points along these barriers which the adversary can go through. The stairwells enable movement from one level of a facility to another.

This is the only phase performed entirely by the user without any use of the computer.

Facility Representation. During this phase, a computer representation of the facility layout is generated using a Tektronix 4050 Series desk-top microcomputer, a Talos digitizer and the Graphical Representation Interactive Digitization (GRID) program. The facility layout is digitized as a series of lines and points later converted by the computer into arcs and nodes.

A coordinate system is set up and the representation is scaled in proportion to actual dimensions of the facility.

The nodes represent the targets, stairwells, and penetration points with locations interpreted by the digitizer. The arcs represent the barriers, with locations interpreted the same way. The nodes also have types associated with them so that each type of component can be represented by a different number. This number is then used later to characterize nodes based on type.

Once entered, the data can be displayed on the screen, corrections made and components added or deleted as necessary. When completed, the file generated is transfered to the main computer for further processing.

Component Performance Selection. During this phase, two characteristics are assigned to the penetration points. The first (time) tells how long it takes for the location to be penetrated. The second (probablility of detection) gives the probability that the security force will detect an adversary at that location.

The data for this phase can be obtained by running a program which uses the TOTAL Data Base Manager for retrieval. The database used contains the characteristics of the barriers and their resistance to different methods of penetration. The data is obtained from the "Barrier Technology Handbook" from Sandia Laboratories or from other sources.

An enhancement that was added is to allow the user to supply times and probabilities of detection for regions of the facility. This allows there to be different travel times for different regions and allows there to be probabilities of detection for area sensors.

Adversary Path Analysis. During this phase, adversary paths are identified which most severely test the security system. The paths are unidirectionally optimized from one node (exterior or target) to another (target or exterior). Identification of one or several critical paths can be requested. The three different measures of system stress can be employed.

Two types of pathfinders are available. The first is deterministic, using a single average value for each facility parameter and identifying optimal paths that correspond to those fixed average values. This pathfinder can minimize time, detection probability or interruption probability. Interruption probability is the probability that the adversary will be detected while the security force still has time to respond before the adversary reaches his target. The Dijkstra-Yen search algorithm is used for finding optimal paths. Figure 2-1 shows a sample run of the minimum interruption version for optimum paths from the boundary nodes to the targets. The second pathfinder is stochastic and uses the minimization of probability of timely detection scheme in a Monte Carlo fashion to sets of facility parameters chosen in accord with distribution functions specified by the user. It ranks the paths found and identifies those it considers most critical. It also identifies those adversary activities which occur with highest frequency in the set of paths which are most critical. The stochastic pathfinder is useful when the component performance data is not precisely known. Figure 2-2 shows a sample run of the minimum interruption version using the same start and terminal nodes. Figure 2-3 shows a sample facility layout with a path display of path 3.

Once paths are generated, changes can be made to the component performance data and paths generated again to see what effect the changes have on the outcome.

Since times and probabilities are output for each path and any point may be selected as a start or terminal node, the deterministic pathfinder may be used to determine how long a given path would take and to find the probability of detection along the path.

Effectiveness Evaluation. During this phase, the paths that have been identified as being most likely to defeat the physical security system are examined further to obtain additional measures of the system's vulnerability to attacks along them.

Up to the point at which the adversaries are confronted by the guards or the adversaries complete their task without a confrontation, SAFE uses the Estimate of Adversary Sequence Interruption (EASI) procedure. The adversary path is treated as a sequence of tasks, each having a mean performance time, its standard deviation, and a probability that the alarm system will detect the adversaries once they have performed the task. EASI also requires estimates of mean guard force response time, its standard deviation, and the probability that the existence of an activated alarm will be communicated to the guard force. These data are combined to produce a cumulative probability that the guard force will confront the adversaries before they have succeeded in their objective. This probability can be shown graphically with two and three dimensional plots. Figure 2-4 shows the list of options available and Figure 2-5 shows a plot of the probability of interruption as a function of response time and probability of detection. EASI carries the scenario to the amount of confrontation of guards and adversaries.

The BRIEF ADVERSARY THREAT LOSS ESTIMATOR (BATLE) model assesses the likely outcome of the ensuing struggle. BATLE is a small-scale engagement model that uses estimated average attrition rates rather than carrying out a detailed simulation of the events of the encounter. BATLE estimates these attrition rates from user-specified assumptions about combatant characteristics and circumstances, including posture, cover, weaponry and firing proficiency, using empirical relationships based on military weapons effectiveness data.

BATLE's attrition rates differ for participants who defend or mount an assault. Circumstances and attrition rates can change and additional guards or attackers can arrive at any time during the course of an engagement. The engagement terminates when specified "absorption rates" have been reached. (In practice this almost always means that either the number of guards or the number of adversaries has become zero.) BATLE calculates a probability that the security force will win the battle. The product of this probability and EASI's probability of interruption is SAFE's measure of overall security system effectiveness for a given critical path. Figure 2-6 shows highlights of a BATLE run and its corresponding summary of effectiveness measures.

SNWS IMPLEMENTATION

Because SAFE represents a sophisticated approach to security system analysis, it requires specific support in the form of computer memory and input/output peripherals.

PROGRAM RUN ARCHITECTURE. The following steps must be performed to run SAFE on the SNWS Interdata 7/32 computer:

(1) A simplified version of the facility layout is prepared by the user containing components to be digitized.

(2) The facility is digitized using the digitization program running in BASIC on the Tektronix 4054 terminal using the Talos digitizer and its graphic cursor.

(3) The facility digitized is evaluated by the user and corrections made until a final version is complete. The BASIC program will then write the data to a tape cartridge.

(4) The data from the cartridge is transferred to the Interdata by the user.

(5) A preprocessor called Automatic Region Extraction Algorithm (AREA) is run on the Interdata to generate facility regions. Information of how well the facility was digitized is provided and corrections may need to be made.

(6) Another preprocessor called UNPREP is run which prepares the input to SAFE using the output from AREA.

(7) SAFE is run. First the pathfinders are run and then the effectiveness evaluation at the user's request. The user continues until all information desired about the facility is obtained.

COMPUTATIONAL REQUIREMENTS. SAFE is made up of many programs, the largest of which requires about 200k bytes of memory. The programs combined use about five megabytes of disk space and the files needed for an average size facility use about a third of a megabyte. The amount of time required to run SAFE can vary depending on a number of factors. Preparing the facility for digitization, beginning with the ship plans, could take a few days to two weeks depending on the complexity and availability of data of the facility. The time required for the digitization process depends on the complexity of the facility and the skill of the user, but normally takes from a day to a week. The pre-processors require between 30 minutes to 90 minutes to run depending on the complexity of the facility and how much simultaneous activity is on the system. Path generation and performance evaluation require between ten and thirty minutes varying with how much output the user wants.

Besides a computer, the following equipment is necessary to run SAFE:

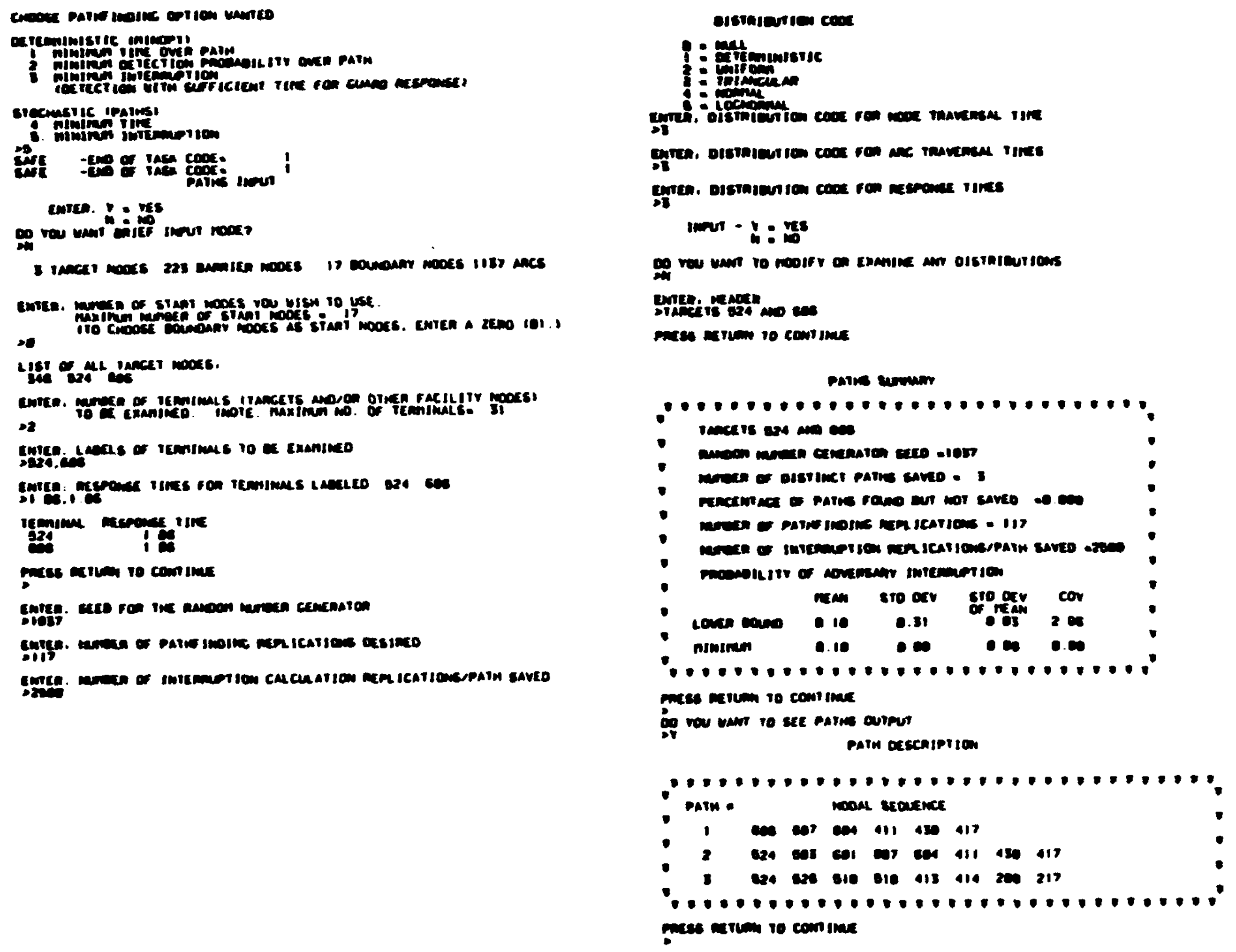
(1) A Tektronix 4050 Series desk-top microcomputer with a tape cartridge. The 4054 is being used for this implementation since its added capabilities enable an improved version of GRID to be run which makes correcting digitization errors relatively easy.

(2) A Talos digitizer connected to the 4054 which contains a twelve button cursor.

(3) A hardcopy unit for making copies of the facility layouts.

```
CHOOSE PATHFINDING OPTION WANTED.

DETERMINISTIC (MINOPT)
  1. MINIMUM TIME OVER PATH
  2. MINIMUM DETECTION PROBABILITY OVER PATH
  3. MINIMUM INTERRUPTION
     (DETECTION WITH SUFFICIENT TIME FOR GUARD RESPONSE)

STOCHASTIC (PATHS)
  4. MINIMUM TIME
  5. MINIMUM INTERRUPTION
>3
STOP
SAFE     -END OF TASK CODE=        0
STOP
SAFE     -END OF TASK CODE=        0
MINIMUM INTERRUPTION PATHFINDING OPTION

MINIMIZE DETECTION PROBABILITY UP TO A LOCUS ABOUT
EACH TERMINAL NODE AND MINIMIZE TIME INSIDE THE LOCUS


   3 TARGET NODES  223 BARRIER NODES   17 BOUNDARY NODES
1137 ARCS          148 REGIONS
THE LIST OF TARGET NODES FOLLOWS.
 348  524  808
HOW MANY START NODES DO YOU WISH TO USE?
(MAXIMUM NUMBER OF START NODES = 17)
TO CHOOSE BOUNDARY NODES AS START NODES, ENTER A ZERO (0).
>0

HOW MANY TERMINALS (TARGETS AND/OR OTHER FACILITY NODES)
WILL BE EXAMINED DURING THIS RUN?
MAXIMUM NUMBER OF TERMINALS =   30
>2

ENTER THE LABELS OF THE TERMINALS TO BE EXAMINED
SEPARATE THEM BY COMMAS.
>524,808

 INPUT RESPONSE TIMES FOR TERMINALS LABELED.
  524  808
 >1.00,1.00

 TERMINAL  RESPONSE TIME
    524            1.00
    808            1.00
 SAFE    -END OF TASK CODE=        0


             VERT EASI   RESP. TIME  TIME  PROB. OF
 PATH NO.     P0(I)     TO TERMINAL  MIN.  DETECTION   PATH DESCRIPTION
    1          0.10          1.00    0.00      0.10    217  209  414  415
                                                       518  519  526  528
                                                       524
    2          0.00          1.00    0.04      0.00    417  430  411  804
                                                       807  601  801  503
                                                       524
    3          0.10          1.00    0.01      0.10    417  430  411  804
                                                       807  807  808

 INPUT PROBABILITY OF COMMUNICATION
 >1

 DO YOU WISH TO DO MULTI-PATH ANALYSIS (TYPE 1)
 OR SINGLE PATH ANALYSIS (TYPE 0)?
 >0

 CHOOSE ONE OF THE CRITICAL PATHS BY ENTERING ITS NUMBER.
 >1

 DO YOU WANT TO DISPLAY THE CRITICAL PATH(S)?
    1 = YES   0 = NO
 >1
```

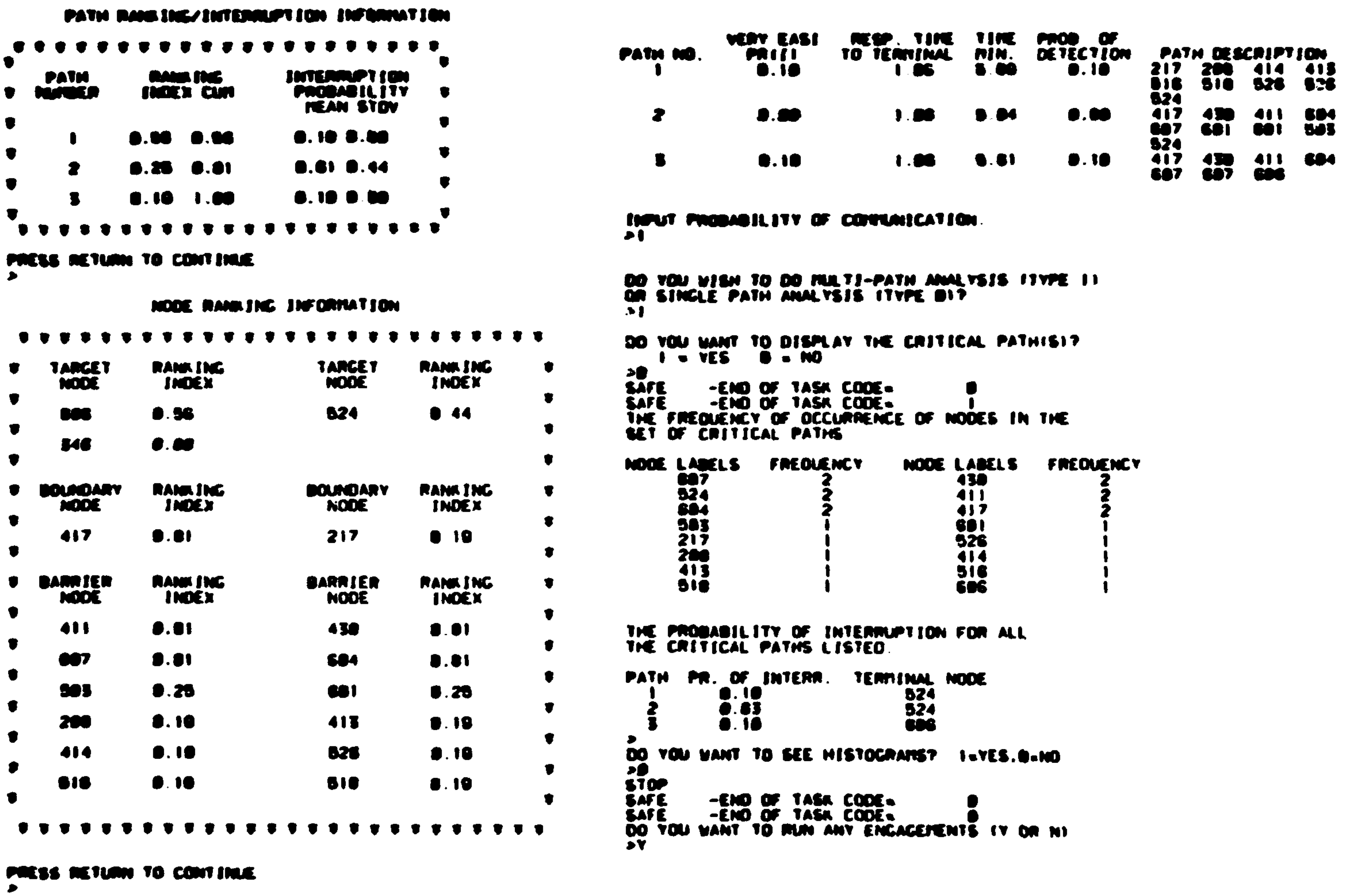
FIGURE 2-1 SAMPLE DETERMINISTIC PATHFINDER RUN



```
CHOOSE PATHFINDING OPTION WANTED

DETERMINISTIC (MINCPT)
   1  MINIMUM TIME OVER PATH
   2  MINIMUM DETECTION PROBABILITY OVER PATH
   3  MINIMUM INTERRUPTION
      (DETECTION WITH SUFFICIENT TIME FOR GUARD RESPONSE)

STOCHASTIC (PATHS)
   4  MINIMUM TIME
   5. MINIMUM INTERRUPTION
>5
SAFE     -END OF TASK CODE=          1
SAFE     -END OF TASK CODE=          1
                        PATHS INPUT

     ENTER. Y = YES
            N = NO
DO YOU WANT BRIEF INPUT MODE?
>N

   3 TARGET NODES  223 BARRIER NODES   17 BOUNDARY NODES 1137 ARCS


ENTER. NUMBER OF START NODES YOU WISH TO USE.
       MAXIMUM NUMBER OF START NODES =  17
       (TO CHOOSE BOUNDARY NODES AS START NODES, ENTER A ZERO (0).)
>0

LIST OF ALL TARGET NODES.
 346  524  806

ENTER. NUMBER OF TERMINALS (TARGETS AND/OR OTHER FACILITY NODES)
       TO BE EXAMINED.  (NOTE. MAXIMUM NO. OF TERMINALS=  3)
>2

ENTER. LABELS OF TERMINALS TO BE EXAMINED
>524,806

ENTER: RESPONSE TIMES FOR TERMINALS LABELED  524  806
>1.06,1.06

TERMINAL  RESPONSE TIME
 524            1.06
 806            1.06

PRESS RETURN TO CONTINUE
>

ENTER. SEED FOR THE RANDOM NUMBER GENERATOR
>1037

ENTER. NUMBER OF PATHFINDING REPLICATIONS DESIRED
>117

ENTER. NUMBER OF INTERRUPTION CALCULATION REPLICATIONS/PATH SAVED
>2000
```

```
          DISTRIBUTION CODE

      0 = NULL
      1 = DETERMINISTIC
      2 = UNIFORM
      3 = TRIANGULAR
      4 = NORMAL
      5 = LOGNORMAL
ENTER, DISTRIBUTION CODE FOR NODE TRAVERSAL TIME
>3

ENTER, DISTRIBUTION CODE FOR ARC TRAVERSAL TIMES
>3

ENTER, DISTRIBUTION CODE FOR RESPONSE TIMES
>3

     INPUT - Y = YES
             N = NO

DO YOU WANT TO MODIFY OR EXAMINE ANY DISTRIBUTIONS
>N

ENTER, HEADER
>TARGETS 524 AND 806

PRESS RETURN TO CONTINUE


                        PATHS SUMMARY

 * * * * * * * * * * * * * * * * * * * * * * * * * * * *
 *                                                      *
 *     TARGETS 524 AND 806                              *
 *                                                      *
 *     RANDOM NUMBER GENERATOR SEED =1037               *
 *                                                      *
 *     NUMBER OF DISTINCT PATHS SAVED =  3              *
 *                                                      *
 *     PERCENTAGE OF PATHS FOUND BUT NOT SAVED  =0.000  *
 *                                                      *
 *     NUMBER OF PATHFINDING REPLICATIONS = 117         *
 *                                                      *
 *     NUMBER OF INTERRUPTION REPLICATIONS/PATH SAVED =2000
 *                                                      *
 *     PROBABILITY OF ADVERSARY INTERRUPTION            *
 *                                                      *
 *                   MEAN    STD DEV    STD DEV    COV  *
 *                                      OF MEAN         *
 *    LOWER BOUND    0.10     0.31       0.03     2.06  *
 *                                                      *
 *    MINIMUM        0.10     0.00       0.00     0.00  *
 *                                                      *
 * * * * * * * * * * * * * * * * * * * * * * * * * * * *

PRESS RETURN TO CONTINUE
>
DO YOU WANT TO SEE PATHS OUTPUT
>Y
                          PATH DESCRIPTION

 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
 *                                                          *
 *  PATH #               NODAL SEQUENCE                     *
 *                                                          *
 *    1      806  807  804  411  430  417                   *
 *                                                          *
 *    2      524  503  601  807  804  411  430  417         *
 *                                                          *
 *    3      524  526  510  518  413  414  200  217         *
 *                                                          *
 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

PRESS RETURN TO CONTINUE
>
```

FIGURE 2-2   SAMPLE STOCHASTIC PATHFINDER



```
           PATH RANKING/INTERRUPTION INFORMATION

 ************************************************
 *  PATH       RANKING          INTERRUPTION    *
 *  NUMBER     INDEX CUM         PROBABILITY    *
 *                                MEAN STDV     *
 *                                              *
 *    1       0.66  0.66        0.10 0.00       *
 *                                              *
 *    2       0.25  0.91        0.81 0.44       *
 *                                              *
 *    3       0.10  1.00        0.10 0.00       *
 *                                              *
 ************************************************
PRESS RETURN TO CONTINUE
>
                 NODE RANKING INFORMATION

 **************************************************************
 *  TARGET     RANKING              TARGET     RANKING        *
 *   NODE       INDEX                NODE       INDEX         *
 *                                                            *
 *   606       0.56                  524       0 44           *
 *                                                            *
 *   546       0.00                                           *
 *                                                            *
 *  BOUNDARY   RANKING              BOUNDARY   RANKING        *
 *   NODE       INDEX                NODE       INDEX         *
 *                                                            *
 *   417       0.81                  217       0 19           *
 *                                                            *
 *  BARRIER    RANKING              BARRIER    RANKING        *
 *   NODE       INDEX                NODE       INDEX         *
 *                                                            *
 *   411       0.81                  430       0.81           *
 *                                                            *
 *   607       0.81                  604       0.81           *
 *                                                            *
 *   503       0.25                  601       0.25           *
 *                                                            *
 *   208       0.10                  413       0.19           *
 *                                                            *
 *   414       0.10                  526       0.10           *
 *                                                            *
 *   518       0.10                  516       0.19           *
 *                                                            *
 **************************************************************

PRESS RETURN TO CONTINUE
>
```

```
              VERY EASI   RESP. TIME   TIME   PROB  OF
PATH NO.        PRI(I     TO TERMINAL  MIN.   DETECTION    PATH DESCRIPTION
   1            0.10          1.06     5.00      0.10      217  208  414  413
                                                           516  518  526  526
                                                           524
   2            0.00          1.06     0.04      0.00      417  430  411  604
                                                           607  601  601  503
                                                           524
   3            0.10          1.06     0.01      0.10      417  430  411  604
                                                           607  607  606

INPUT PROBABILITY OF COMMUNICATION.
>1

DO YOU WISH TO DO MULTI-PATH ANALYSIS (TYPE 1)
OR SINGLE PATH ANALYSIS (TYPE 0)?
>1

DO YOU WANT TO DISPLAY THE CRITICAL PATH(S)?
   1 = YES   0 = NO
>0
SAFE    -END OF TASK CODE=       0
SAFE    -END OF TASK CODE=       1
THE FREQUENCY OF OCCURRENCE OF NODES IN THE
SET OF CRITICAL PATHS

NODE LABELS   FREQUENCY    NODE LABELS   FREQUENCY
     607          2            430           2
     524          2            411           2
     604          2            417           2
     503          1            601           1
     217          1            526           1
     208          1            414           1
     413          1            516           1
     518          1            606           1

THE PROBABILITY OF INTERRUPTION FOR ALL
THE CRITICAL PATHS LISTED.

PATH  PR. OF INTERR.  TERMINAL NODE
  1       0.10             524
  2       0.83             524
  3       0.10             606
>
DO YOU WANT TO SEE HISTOGRAMS?  1=YES.0=NO
>0
STOP
SAFE    -END OF TASK CODE=       0
SAFE    -END OF TASK CODE=       0
DO YOU WANT TO RUN ANY ENGAGEMENTS (Y OR N)
>Y
```

FIGURE 2-2 SAMPLE STOCHASTIC PATHFINDER (CONTINUED)

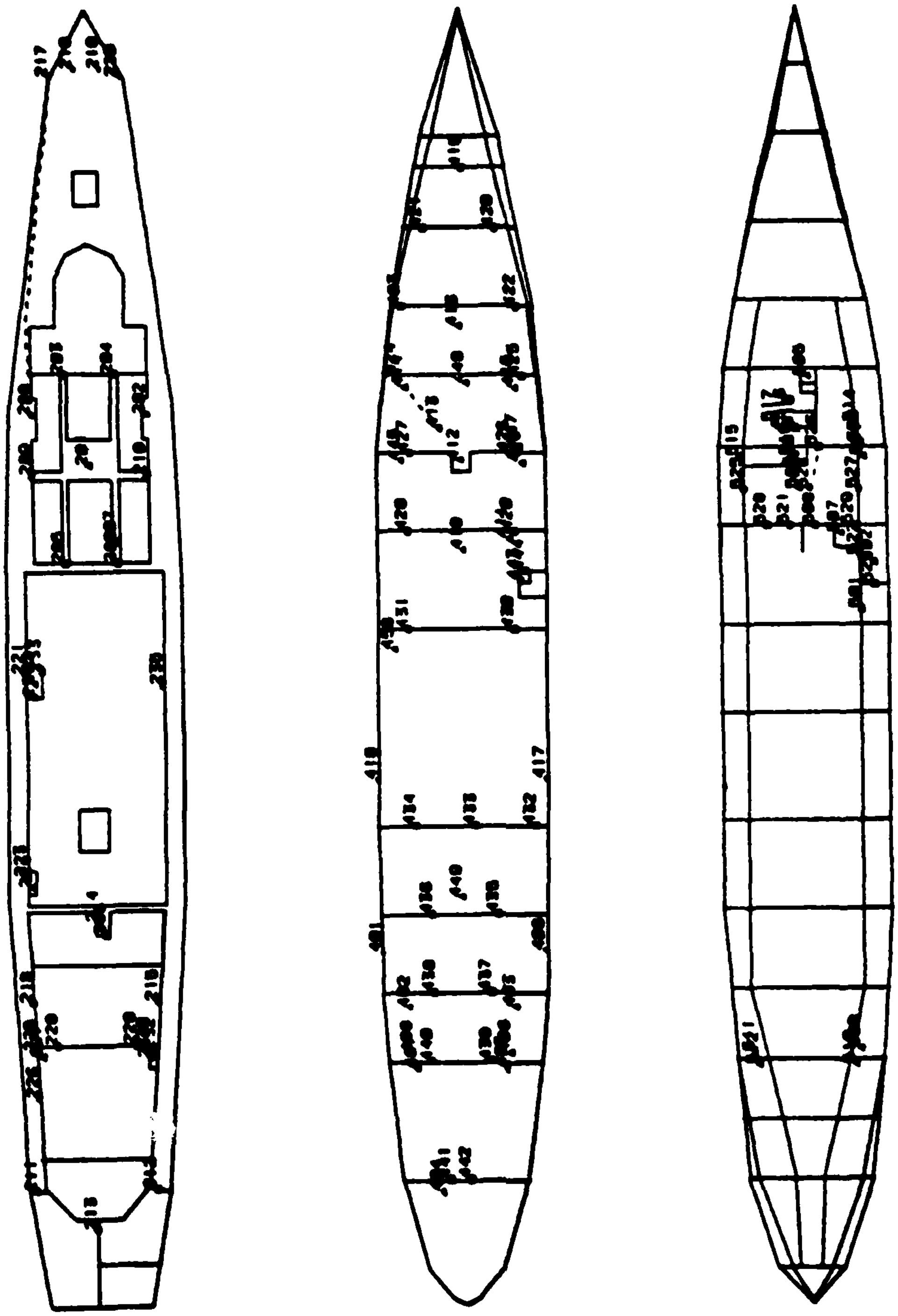


FIGURE 2-3 SAMPLE PATH DISPLAY

```
    PROBABILITY OF ADVERSARY INTERRUPTION = 0.103
    PROBABILITY OF SYSTEM VIN = 0.103
PRESS RETURN TO CONTINUE
>
PLOTS DESIRED? 1=YES. 0=NO   RETURN
>1
NEED CURRENT DATA LISTED? 1=YES.0=NO   RETURN
>0
NEED PLOT OPTIONS LISTED? 1=YES.0=NO   RETURN
>1
PLOT OPTIONS
     0   NO PLOT
     1   PROBABILITY OF ALARM VS. TIME TO TERMINAL POINT
     2   PROBABILITY OF INTERRUPTION VS. TIME TO TERMINAL POINT

          PROBABILITY OF INTERRUPTION OR SYSTEM VIN VS.
     3   RESPONSE TIME
     4   PROBABILITY OF COMMUNICATION
     5   TASK TIME
     6   PROBABILITY OF DETECTION

 PROBABILITY OF INTERRUPTION OR SYSTEM VIN AS A FUNCTION OF
     7   RESPONSE TIME AND PROBABILITY OF COMMUNICATION
     8   TASA TIME AND PROBABILITY OF DETECTION
     9   RESPONSE TIME AND TASA TIME
    10   RESPONSE TIME AND PROBABILITY OF DETECTION
    11   PROBABILITY OF COMMUNICATION AND PROBABILITY OF DETECTION
    12   TASA TIME AND PROBABILITY OF COMMUNICATION
    13   TASA TIME AND TASA TIME
    14   PROBABILITY OF DETECTION AND PROBABILITY OF DETECTION


 PROBABILITY OF SYSTEM VIN AS A FUNCTION
 OF PROBABILITY OF NEUTRALIZATION AND
    15   RESPONSE TIME
    16   PROBABILITY OF COMMUNICATION
    17   TASA TIME
    18   PROBABILITY OF DETECTION

ENTER PLOT OPTION NUMBER   RETURN
>10
WHICH DEPENDENT VARIABLE?
     1   PROBABILITY OF INTERRUPTION
     2   PROBABILITY OF SYSTEM VIN
ENTER NUMBER OF CHOICE      RETURN
>1
DO YOU WANT DATA DISPLAYED ON PLOT? 1=YES,0=NO   RETURN
>0
ENTER RATIO OF MEAN RESPONSE TIME TO STANDARD DEVIATION   RETURN
>6

WHICH SENSOR IS THE VARIABLE?
ENTER SENSOR NUMBER   RETURN
>2
DO YOU WANT TO SET YOUR OWN SCALE?1=YES,0=NO    RETURN
>0
```

FIGURE 2-4 SAMPLE EASI RUN

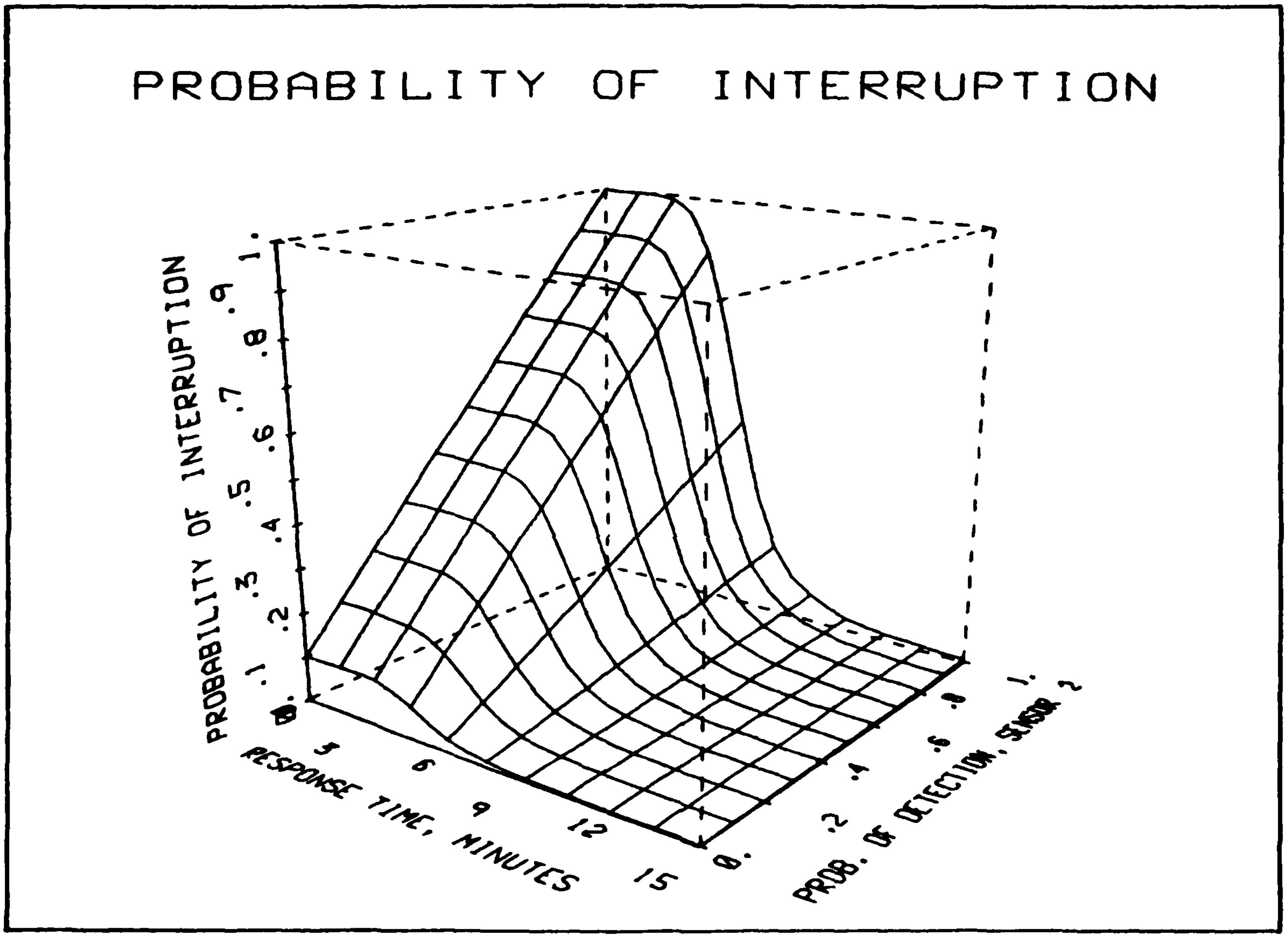
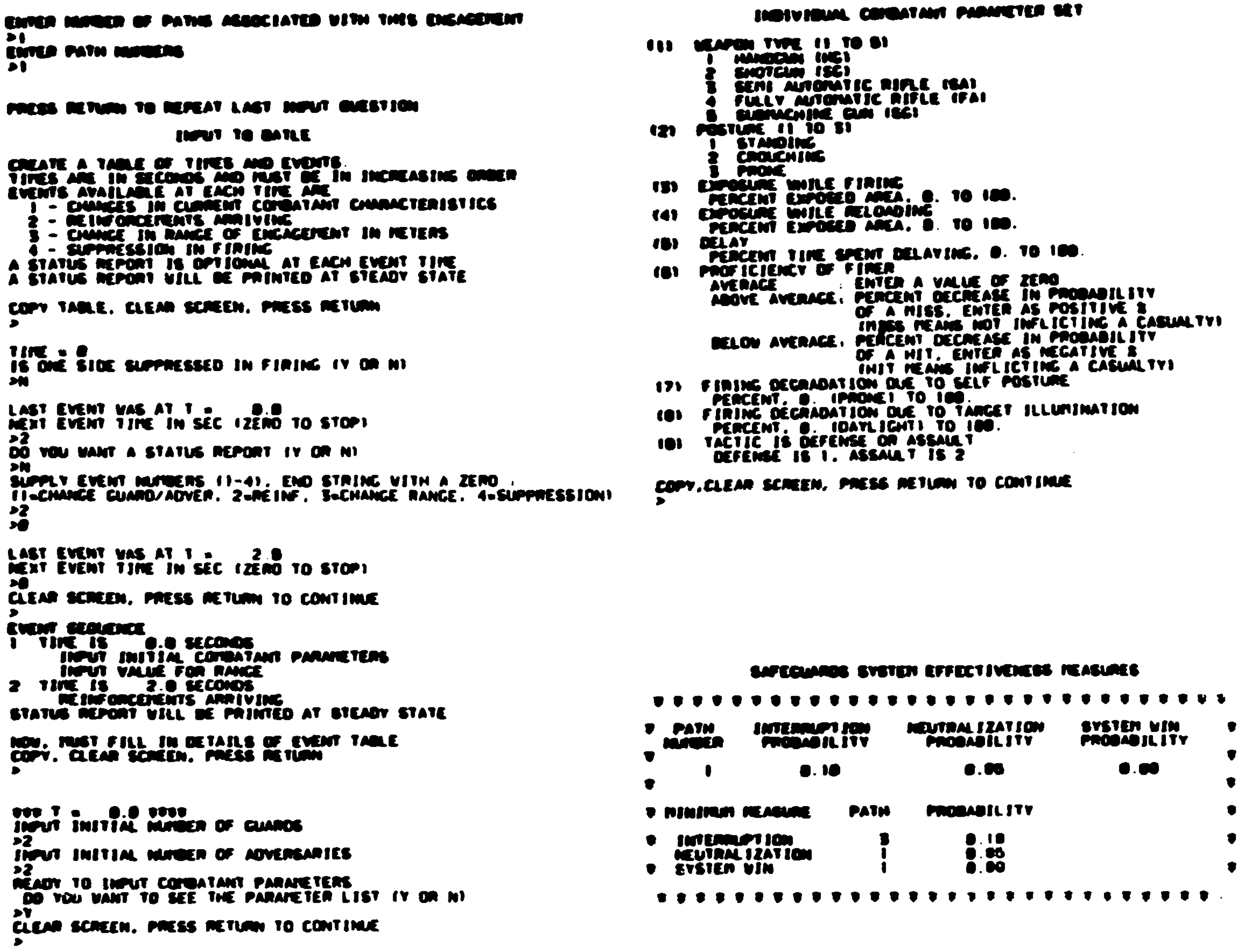


FIGURE 2-5 SAMPLE EASI GRAPHICS



```
ENTER NUMBER OF PATHS ASSOCIATED WITH THIS ENGAGEMENT
>1
ENTER PATH NUMBERS
>1

PRESS RETURN TO REPEAT LAST INPUT QUESTION

                 INPUT TO BATLE

CREATE A TABLE OF TIMES AND EVENTS.
TIMES ARE IN SECONDS AND MUST BE IN INCREASING ORDER
EVENTS AVAILABLE AT EACH TIME ARE
   1 - CHANGES IN CURRENT COMBATANT CHARACTERISTICS
   2 - REINFORCEMENTS ARRIVING
   3 - CHANGE IN RANGE OF ENGAGEMENT IN METERS
   4 - SUPPRESSION IN FIRING
A STATUS REPORT IS OPTIONAL AT EACH EVENT TIME
A STATUS REPORT WILL BE PRINTED AT STEADY STATE

COPY TABLE. CLEAR SCREEN. PRESS RETURN
>

TIME = 0
IS ONE SIDE SUPPRESSED IN FIRING (Y OR N)
>N

LAST EVENT WAS AT T =    0.0
NEXT EVENT TIME IN SEC (ZERO TO STOP)
>2
DO YOU WANT A STATUS REPORT (Y OR N)
>N
SUPPLY EVENT NUMBERS (1-4). END STRING WITH A ZERO .
(1=CHANGE GUARD/ADVER. 2=REINF. 3=CHANGE RANGE. 4=SUPPRESSION)
>2
>0

LAST EVENT WAS AT T =    2.0
NEXT EVENT TIME IN SEC (ZERO TO STOP)
>0
CLEAR SCREEN, PRESS RETURN TO CONTINUE
>
EVENT SEQUENCE
1  TIME IS     0.0 SECONDS
     INPUT INITIAL COMBATANT PARAMETERS
     INPUT VALUE FOR RANGE
2  TIME IS     2.0 SECONDS
     REINFORCEMENTS ARRIVING
STATUS REPORT WILL BE PRINTED AT STEADY STATE

NOW, MUST FILL IN DETAILS OF EVENT TABLE
COPY. CLEAR SCREEN. PRESS RETURN
>


*** T =   0.0 ****
INPUT INITIAL NUMBER OF GUARDS
>2
INPUT INITIAL NUMBER OF ADVERSARIES
>2
READY TO INPUT COMBATANT PARAMETERS
 DO YOU WANT TO SEE THE PARAMETER LIST (Y OR N)
>Y
CLEAR SCREEN. PRESS RETURN TO CONTINUE
>
```

```
            INDIVIDUAL COMBATANT PARAMETER SET

(1)  WEAPON TYPE (1 TO 5)
      1  HANDGUN (HG)
      2  SHOTGUN (SG)
      3  SEMI AUTOMATIC RIFLE (SA)
      4  FULLY AUTOMATIC RIFLE (FA)
      5  SUBMACHINE GUN (SG)
(2)  POSTURE (1 TO 3)
      1  STANDING
      2  CROUCHING
      3  PRONE
(3)  EXPOSURE WHILE FIRING
      PERCENT EXPOSED AREA, 0. TO 100.
(4)  EXPOSURE WHILE RELOADING
      PERCENT EXPOSED AREA, 0. TO 100.
(5)  DELAY
      PERCENT TIME SPENT DELAYING, 0. TO 100.
(6)  PROFICIENCY OF FIRER
      AVERAGE       : ENTER A VALUE OF ZERO
      ABOVE AVERAGE, PERCENT DECREASE IN PROBABILITY
                     OF A MISS, ENTER AS POSITIVE %
                     (MISS MEANS NOT INFLICTING A CASUALTY)
      BELOW AVERAGE, PERCENT DECREASE IN PROBABILITY
                     OF A HIT, ENTER AS NEGATIVE %
                     (HIT MEANS INFLICTING A CASUALTY)
(7)  FIRING DEGRADATION DUE TO SELF POSTURE
      PERCENT, 0. (PRONE) TO 100.
(8)  FIRING DEGRADATION DUE TO TARGET ILLUMINATION
      PERCENT, 0. (DAYLIGHT) TO 100.
(9)  TACTIC IS DEFENSE OR ASSAULT
      DEFENSE IS 1, ASSAULT IS 2

COPY,CLEAR SCREEN, PRESS RETURN TO CONTINUE
>
```

```
          SAFEGUARDS SYSTEM EFFECTIVENESS MEASURES

 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
 *  PATH    INTERRUPTION    NEUTRALIZATION    SYSTEM WIN    *
   NUMBER   PROBABILITY      PROBABILITY     PROBABILITY
 *                                                          *
      1        0.10             0.05             0.00
 *                                                          *
 * MINIMUM MEASURE      PATH     PROBABILITY                *
 *   INTERRUPTION         3         0.10                    *
     NEUTRALIZATION       1         0.05
 *   SYSTEM WIN           1         0.00                    *
 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

FIGURE 2-6 SECTIONS OF A SAMPLE DATE RUN AND SUMMARY OF EFFECTIVENESS MEASURES

REFERENCES

2-1) Chapman, L.D., Engi D., Grady, L.M., and Pavlakos, C., "SAFE USERS MANUAL. VOLUME I: EXECUTIVE SUMMARY," Sandia Laboratories, Albuquerque, New Mexico, Aug. 1980.

2-2) Chapman, L.D., Engi D., Grady, L.M., and Pavlakos, C., "SAFE USERS MANUAL. VOLUME II: METHOD DESCRIPTION," Sandia Laboratories, Albuquerque, New Mexico, Aug. 1980.

2-3) Chapman, L.D., Engi D., Grady, L.M., and Pavlakos, C., "SAFE USERS MANUAL. VOLUME III: EXAMPLE APPLICATION," Sandia Laboratories, Albuquerque, New Mexico, Aug. 1980.

2-4) Davidson, R.B., and Rosengren, J.W.,"Current Methods for Evaluation of Physical Security System Effectiveness," R and D Associates, Arlington, Virginia, May 1981.

2-5) Engi, D., and Harlan, C.P., "BRIEF ADVERSARY THREAT LOSS ESTIMATOR (BATLE) USER'S GUIDE," Sandia Laboratories, Albuquerque, New Mexico, March 1981.

2-6) Sasser, D.W., "EASI Graphics--GCS Version,"Sandia Laboratories, Albuquerque, New Mexico, March 1980.

2-7) Schwartz, M.S., "THE SAFEGUARDS AUTOMATED FACILITY EVALUATION (SAFE) ON THE INTERDATA 7/32," NSWC TR 81-321, Aug. 1981.

CHAPTER 3

SNAP

INTRODUCTION

In the previous chapter the Safeguards Automated Facility Evaluation (SAFE) model was discussed. There it was shown that limited control was available to the user when specifying the tactics of the personnel at the facility such as specifying minimum interruption. The model is therefore concerned primarily with the facility and does not place major emphasis on the tactics of the personnel that use it.

The Safeguards Network Analysis Procedure (SNAP) model was developed to place more emphasis on the personnel. This includes both adversaries, guards, and even guards turned traitor (insiders). To be sure, the same facility as evaluated by SAFE must be known to SNAP. However, the results of the model depends primarily on the tactics of the personnel using the facility rather than the facility itself.

The SNAP model is an event driven network model developed by Pritsker and Associates, Inc., West Lafayette, Indiana under subcontract from Sandia National Laboratories, Albuquerque, New Mexico. Early funding in the models development was provided by the Nuclear Regulatory Commission whereas the more recent enhancements have been funded by the Naval Surface Weapons Center. The model has been in development over the last five years and is now being used to analyze the security of ships, reactors, and fuel processing and storage facilities.

An upgrade in the SNAP model has made it possible to extract the facility data of the SAFE model. To do so, the model user interfaces with the Snap Operating System (SOS) and by issuing certain procedural commands instructs SOS to make the translation. This produces a skeletal input network for SNAP and, if run, gives results like those observed in SAFE. The advantage of the SOS system is that the user can add more detail or content to this input by using the utilities that SOS provides or he can design model networks using SOS exclusively independent of SAFE. SNAP therefore now consists of the modeling tool itself, along with its own operating system to assist the user in assembling the required input.

The model can perform tasks which include moving from place to place, penetrating barriers, sabotaging nuclear material, and defeating or sabotoging of sensors. All may be done in a probabilistic manner, if desired, which means that in some runs they are not done at all. The forces move through the facility and interact realistically with each other. Some tasks can be triggered by other events. An example of this would be an adversary engaging a guard as soon as the guard shows up. Forces may split, merge, appear, and disappear. Accordingly, a guard can dissappear and an adversary appear in his place to effectively model a guard turned traitor. While he's a guard, he performs his normal duties with his true identity concealed. Another technique that could be used to model the insider is to have a phantom adversary track along with the guard in such a manner that an engagement did not occur. The phantom adversary could be performing the insider's covert acts. This type of modeling, however, places an extra burden on the user to keep track of everything. In most cases, the insider can be effectively modeled simply by not allowing him to enter into an engagement. This is done by not including the "engagement continue" parameter on the desired nodes. Therefore, even though more difficult to do, the model can adequately handle the insider threat. This is made possible by the model's ability to adapt to most situations. In general most safeguard's threat or situation can be modeled with SNAP.

PROBLEM ADDRESSED

The SNAP model was developed as a tool to assist the analyst in evaluating a facility given the wide spectrum of guard tactics and adversary ingenuity that we know exists. Consequently, the model is a powerful tool that will help analyze existing guard tactics, sensors, and barriers, as well as proposed changes to them. The model is, therefore, scenario specific and has practically no limit to the amount of detail that may be included.

DESCRIPTION OF THE MODELING APPROACH

SYMBOLOGY. The SNAP modeling approach includes a network symbology which represents event transactions and facility locations. The user combines these network symbols in various ways and thereby develops the specific scenario of interest. The user must therefore have knowledge of the facility and its safeguard objectives.

Once the network symbols have been arranged into the desired scenario, they are translated into the models input procedural language. This is done by the user with or without the help of the SOS. As mentioned earlier, SOS has the capability of producing a skeletal SNAP input network from a prior SAFE run. The network is skeletal in the sense that the user may build upon it to produce the desired scenario, but in reality it is a detailed description of the facility, scenario, and threat as observed by SAFE. This is of great assistance to the user who can then use the SOS utilities to edit, store, and retrieve this input as he adds detail. The SOS editor also includes the capability of merging chunks or building blocks of standard scenario. More important, however, is the fact that this input development is done using graphical symbols that portray the scenario more vividly to the user than would be apparent from a line of input code. Making the task of input preparation easier was one of the primary reasons for developing the SOS.

To summarize, the SNAP modeling method normally consists of the following steps:

(1) Perform a SAFE analysis of the facility as described in Chapter 2.

(2) Translate the data files of SAFE into a skeletal SNAP network using SOS.

(3) Edit the model to the desired scenario using the SOS (i. e., produce the modified SNAP input network).

(4) Run the SNAP model.

(5) Analyze the SNAP output reports and/or traces from the run. If necessary, go back to number three and repeat.

SNAP DESCRIPTION.

Input Requirements. The SNAP input consists of a set of commands that a new user can learn in several days to a week. Its degree of difficulty may be compared to learning a new computer language such as BASIC or FORTRAN. That is, one can start writing simple input codes very early in the learning process, but to become proficient would normally require several months. In addition, the user should be familiar with statistics to understand the output reports as well as be able to specify some of the input distributions that determine the various task times. An additional feature of the model allows the user to write a user function in FORTRAN, link it with the model, and thus be able to model more complex situations. This is for the advanced user, however, and may be used infrequently since many situations can be handled without it.

The input can be broken up into three major subgroups: the facility network, the guard network, and the adversary network. The guard and adversary networks are completely independent from one another and can therefore be thought out or developed separately. It's not until the SNAP program is run that these networks interact.

In developing the input to SNAP, the user can expect to spend from an hour to perhaps a week or more as he adds the intricate detail of a large scenario. The model does provide syntax diagnostics to assist the user in identifing errors in the scenario. The user may wish to establish a benchmark scenario, then selectively refine it until the desired details are included. In this way error sources are usually constrained to those areas being enhanced.

Fortunately, the SOS does produce many of the input commands automatically, but one or two commands have no symbol counterpart. These commands must therefore be input as text. Overall, because SOS is based on the procedural language, the user is required to know at least a working subset of the complete input language.

An example of the input network symbology will be found in figures 3-1, 3-2, and 3-3. Figure 3-1 represents one of the deck levels of a ship where nuclear material is stored in an exclusion area. The target node, from the adversaries point of view, is labelled SUCC (i.e., they will be successful if they reach it). The actual label used is determined by the analyst and is subject only to the restriction that it be four characters beginning with a letter.

Figure 3-2, an example of a guard network, shows where five guards are allocated. They first stand by and wait for the detection of adversaries by monitor M. When a detection does occur, the guards travel to the exclusion area and enter (taking 1.4 minutes). There they engage any adversaries that arrive. If they win the engagement, assuming the adversaries show up, they exit the network.

Figure 3-3, an example of an adversary network, is simply a series of tasks whereby an adversary is attempting to reach node SUCC. The nodes prior to the last five refer to nodes on different deck levels and therefore would be found on different facility drawings portraying those deck levels.

The network symbology is very easy to understand. The guard network portrays, at a glance, the total task plan of the five guards independent of the adversary network. In a similar manner, the adversary network which describes the adversary task plan is independent of the guard network. Both networks (or plans) are developed separately with the possible exception of consideration given to wait node triggering by opposing forces.

When the model is run, engagements between guards and adversaries might occur if allowed by the input specifications. These specifications are quite flexible. It is even possible to have guards and adversaries at the same location and not trigger an engagement. In this way the model simulates perfect cover. If an engagement does occur, SNAP models it with a discreet stochastic form of the BATLE model similar to the version used in SAFE. The engagements that do occur will terminate as per the specified conditions and the remaining forces will continue on their task plans.

The user will find that the model is capable of handling quite complex relationships between guards and adversaries. In some cases this may require considerable experience on the part of the user. This will be most apparent on large scenarios where the beginning modeler may choose a poor network to model a situation. This, in turn, may produce excessive run times in addition to using excessive amounts of memory. Based on user training and experience, these problems can be minimized.

Output Description. The SNAP model is a Monte Carlo approach. As such, the model is run many times using random draws from probability distributions. The results of these runs are combined to produce the output reports that give, among other things, the statistics of system win or fail. The number of runs is user determined and in essence determines the degree of confidence one has in the results.

The usual practice in statistical calculations of this type is to say that the model result Pw, for probability of system win, lies centered in a range of values that will include the true value a large percentage of the time. This large percentage of the time is commonly taken to be 95% and, once set, determines the width of this range of values. The upper and lower width of this band is a function of the number of Monte Carlo runs, and can be shown to be approximately equal to the reciprocal square root of N.

The total output of the model is, however, actually much more extensive than just determining the probability of system win. It can include, for example, traces of the scenario runs. These are extremely useful in verifying that the model is performing properly. To be more specific, figures 3-4 to 3-6 show representative examples of SNAP output. Figure 3-4 shows a trace of guards and forces moving through a network. The engagements and casualties are listed as they occur. Figure 3-5 lists the results of the Monte Carlo run. Figure 3-6 lists the statistics concerning the facility. This should be analyzed in conjunction with the trace to guarantee that the model is performing properly since it summarizes all runs whereas each trace depicts only one run.

SNAP IMPLEMENTATION

SNAP, as installed at the Naval Surface Weapons Center, requires approximately 160k to 200k bytes of memory depending on the size of the input buffer array called NSET. The model is installed on an Interdata 7/32 which has the Perkin-Elmer Fortran VII optimizing compiler. The later enhancements of SNAP and SOS utilize a compiler that complies with the ANSI 77 standard. One machine dependency exists which is related to the word length. It is the random number generator and can be easily replaced with one designed for the target machine.

The running time varies from a few minutes to hours depending on the number of Monte Carlo runs and scenario complexity. The program, once started, does not require user intervention, and therefore permits queing up of several input scenarios in batch mode.

The program is arranged in a simple overlay structure using a root and two overlays. The SOS is more complex in that it consists of additional levels in the overlays. Consequently, the SOS requires a multilevel overlay processor with a linker which supports the overlay structure.

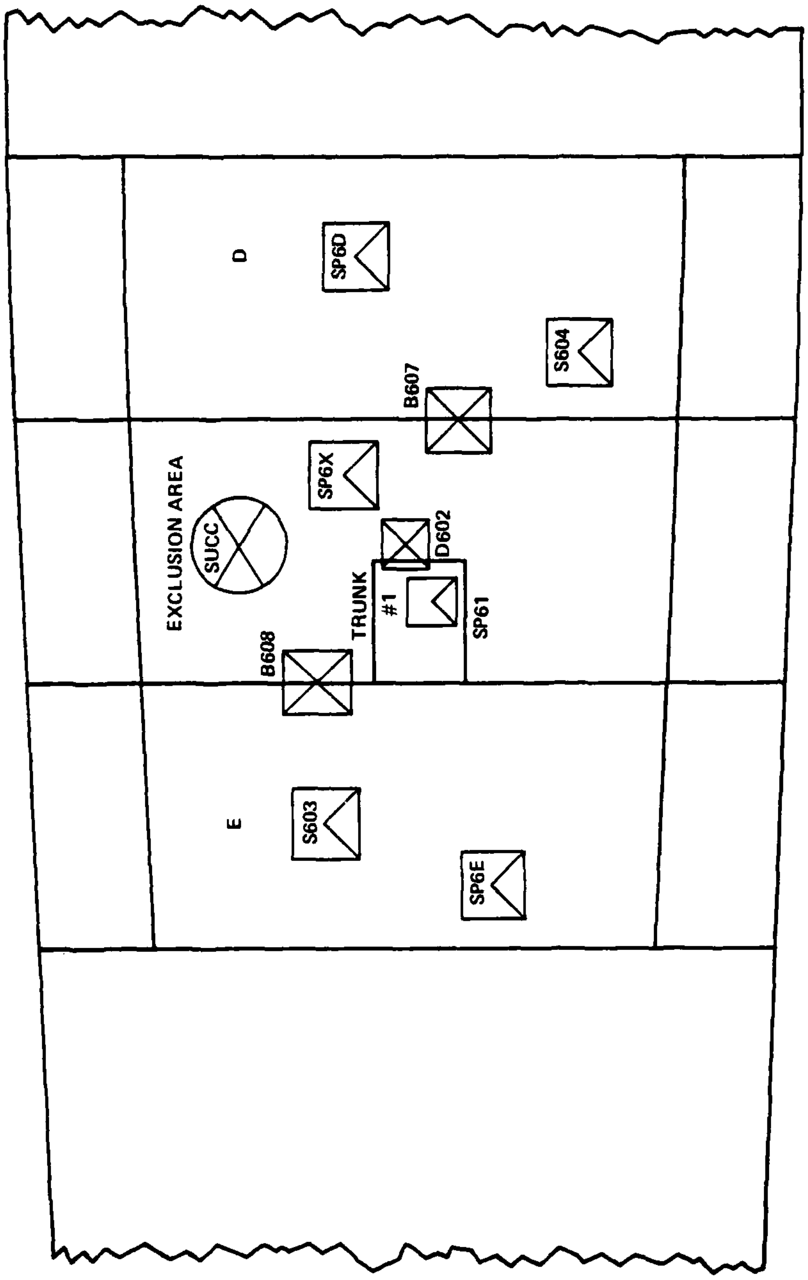


FIGURE 3-1 FACILITY NODE DIAGRAM

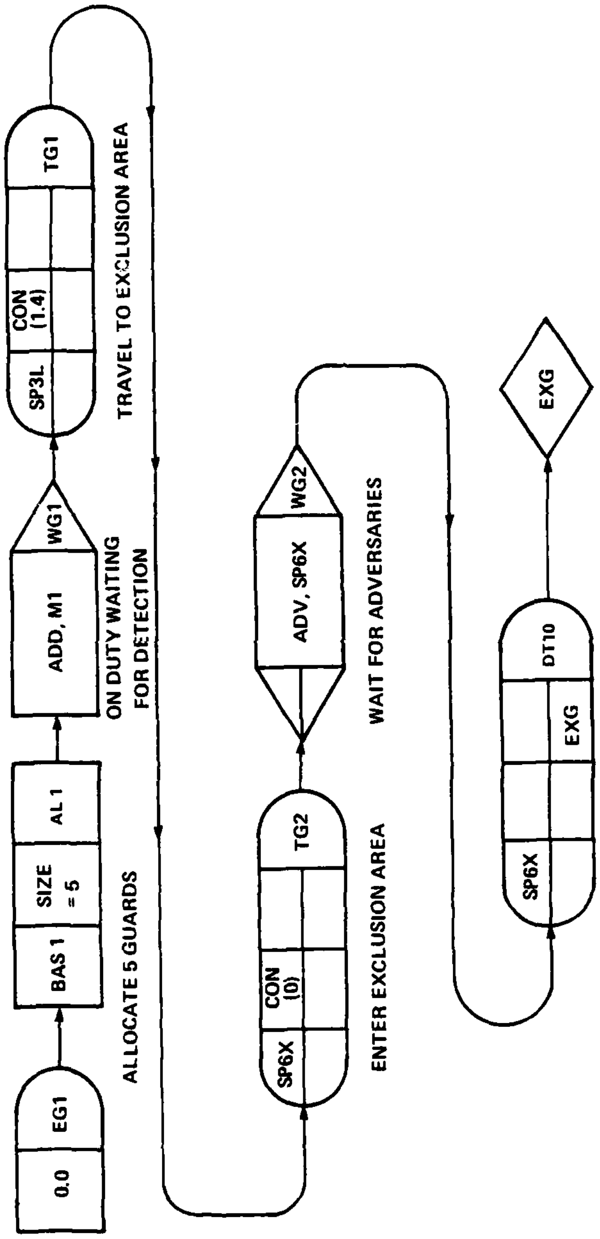


FIGURE 3-2 GUARD SUBNETWORK

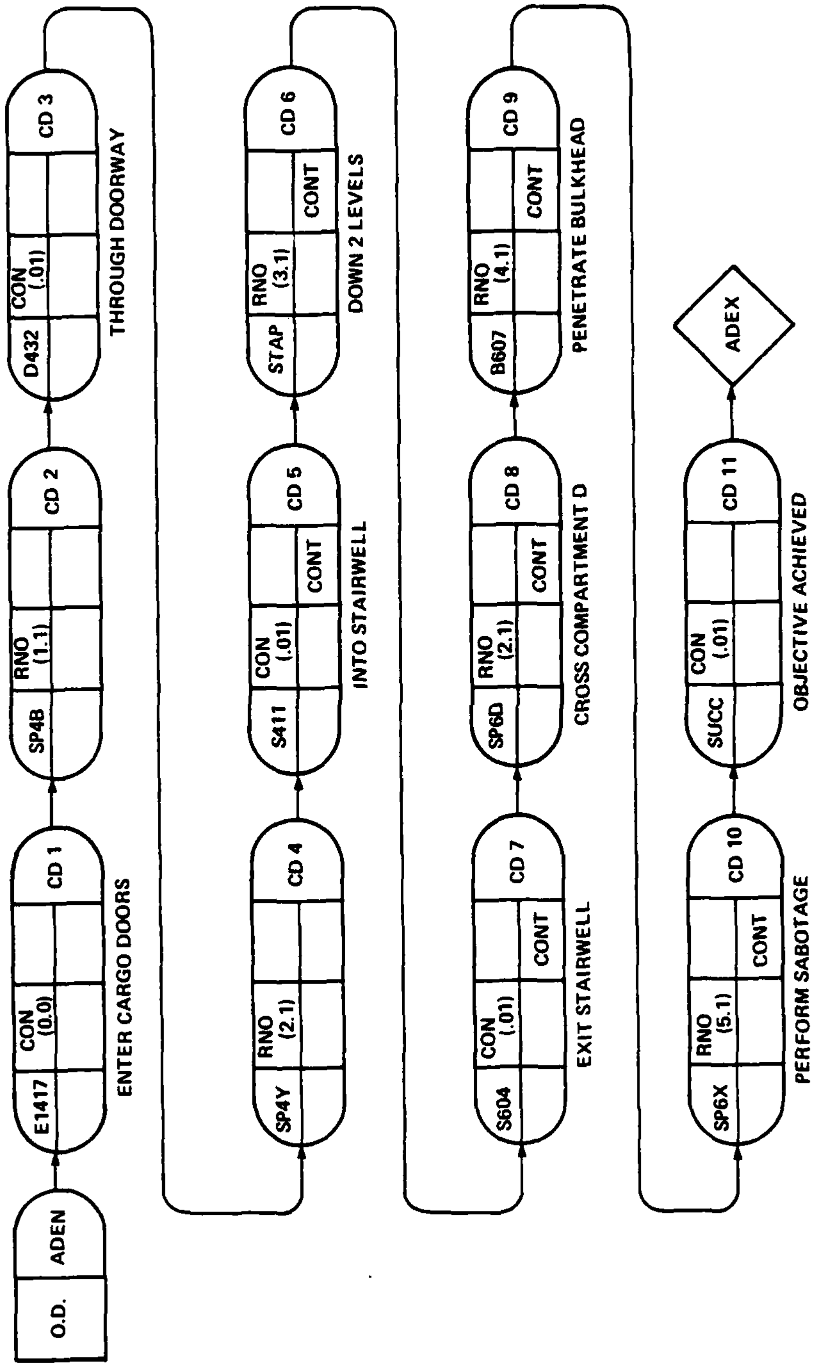
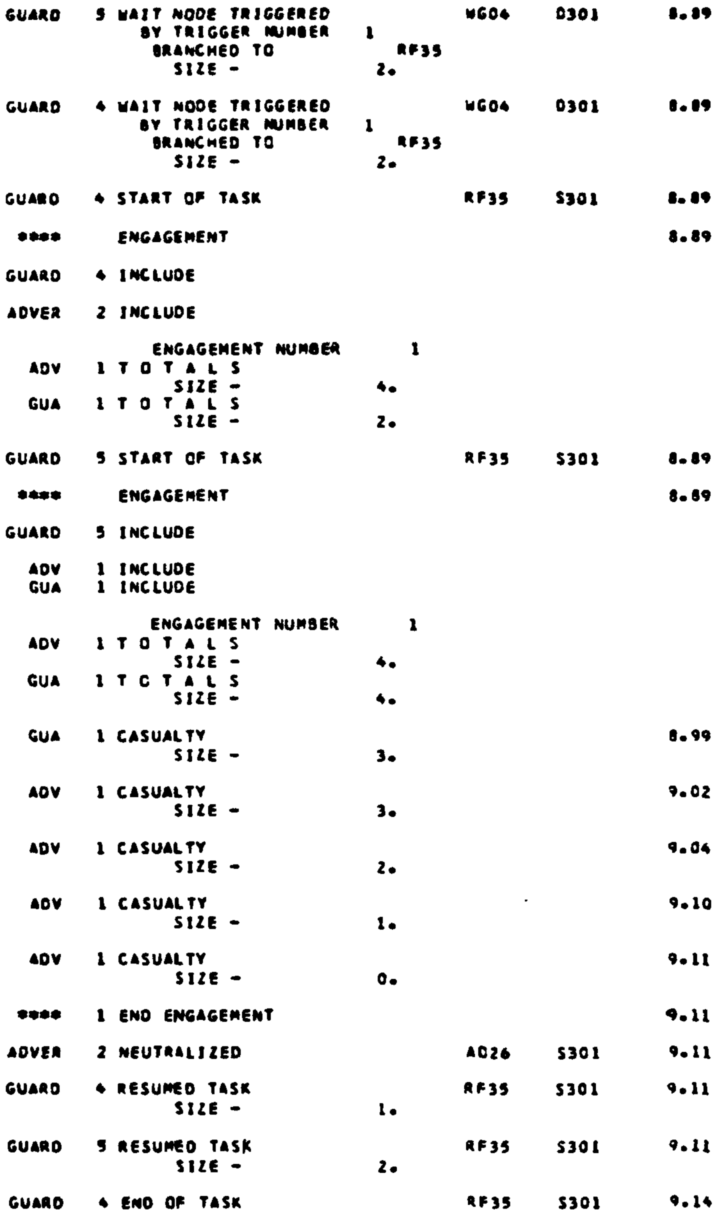


FIGURE 3-3 ADVERSARY SUBNETWORK



```
GUARD   5 WAIT NODE TRIGGERED             WG04    D301       8.89
            BY TRIGGER NUMBER    1
             BRANCHED TO           RF35
               SIZE -             2.

GUARD   4 WAIT NODE TRIGGERED             WG04    D301       8.89
            BY TRIGGER NUMBER    1
             BRANCHED TO           RF35
               SIZE -             2.

GUARD   4 START OF TASK                   RF35    S301       8.89

 ****     ENGAGEMENT                                         8.89

GUARD   4 INCLUDE

ADVER   2 INCLUDE

             ENGAGEMENT NUMBER       1
  ADV   1 T O T A L S
               SIZE -             4.
  GUA   1 T O T A L S
               SIZE -             2.

GUARD   5 START OF TASK                   RF35    S301       8.89

 ****     ENGAGEMENT                                         8.89

GUARD   5 INCLUDE

  ADV   1 INCLUDE
  GUA   1 INCLUDE

             ENGAGEMENT NUMBER       1
  ADV   1 T O T A L S
               SIZE -             4.
  GUA   1 T C T A L S
               SIZE -             4.

  GUA   1 CASUALTY                                           8.99
               SIZE -             3.

  ADV   1 CASUALTY                                           9.02
               SIZE -             3.

  ADV   1 CASUALTY                                           9.04
               SIZE -             2.

  ADV   1 CASUALTY                                           9.10
               SIZE -             1.

  ADV   1 CASUALTY                                           9.11
               SIZE -             0.

 ****   1 END ENGAGEMENT                                     9.11

ADVER   2 NEUTRALIZED                     AD26    S301       9.11

GUARD   4 RESUMED TASK                    RF35    S301       9.11
               SIZE -             1.

GUARD   5 RESUMED TASK                    RF35    S301       9.11
               SIZE -             2.

GUARD   4 END OF TASK                     RF35    S301       9.14
```

FIGURE 3-4 PORTION OF SNAP TRACE

```
                              CASE 1



             ***********************************************
             *                                             *
             *  GENERAL SYSTEM PERFORMANCE STATISTICS     *
             *                                             *
             ***********************************************



                      MEAN  STANDARD  STAND DEV MINIMUM MAXIMUM  NUM OF
                      VALUE DEVIATION  OF MEAN   VALUE   VALUE    OBS.
-----------------------------------------------------------------------

NO. GUARD CSLTY       3.68Ø    1.988    .Ø27     Ø.ØØØ   5.ØØØ     75
NO. ADVER CSLTY       1.1Ø7    1.226    .Ø16     Ø.ØØØ   3.ØØØ     75
DEG OBJ SATISFD        .76Ø     .43Ø    .ØØ6     Ø.ØØØ   1.ØØØ     75
TIME FOR ENG           .677     .442    .ØØ7      .1Ø7   2.383     67
TOTAL ENG TIME         .6Ø4     .467    .ØØ6     Ø.ØØØ   2.383     75
NO. ENG/RUN            .893     .311    .ØØ4     Ø.ØØØ   1.ØØØ     75
TIME BET ENT/ENG      4.366     .765    .Ø11     2.922   5.997     67
SIMULATION TIME       5.772    1.Ø5Ø    .Ø14     3.634   8.266     75
SIM TIME/AD SUC       6.Ø38     .957    .Ø17     3.634   8.266     57
SIM TIME/AD FAIL      4.929     .891    .Ø5Ø     3.779   6.746     18



    AVG NUMBER OF ENGAGEMENTS PER RUN                         .89

    AVG NUMBER OF ENGAGEMENTS WON BY GUARDS PER RUN           .24

    AVG NUMBER OF ENGAGEMENTS WON BY ADVERSARIES              .65

    PROBABILITY SYSTEM WINS                                   .24

    PROBABILITY AN INTERRUPT OCCURS                           .89
```

FIGURE 3-5 SYSTEM PERFORMANCE STATISTICS

```
                    ******************************
                    *                            *
                    *    FACILITY STATISTICS     *
                    *                            *
                    ******************************

               **   STATISTICS FOR FACILITY NODES   **

        PROBABILITY    NUMBER OF TIMES OCCUPIED BY ADVERSARIES PER RUN
        NODE WAS      ------------------------------------------------
NODE    REACHED AT                  STANDARD       STD. DEV.    NO. OF
LABEL   LEAST ONCE        MEAN      DEVIATION      OF MEAN       OBS.
----------------------------------------------------------------------

S501      1.00000       2.00000      0.00000       0.00000          1
S502      1.00000       1.00000      0.00000       0.00000          1
D501      1.00000       2.00000      0.00000       0.00000          1
L541      1.00000       2.00000      0.00000       0.00000          1
S401      1.00000       2.00000      0.00000       0.00000          1
L431      1.00000       2.00000      0.00000       0.00000          1
S301      1.00000       2.00000      0.00000       0.00000          1
S302      1.00000       1.00000      0.00000       0.00000          1
S303      1.00000       1.00000      0.00000       0.00000          1
D301      1.00000       1.00000      0.00000       0.00000          1
D302      1.00000       1.00000      0.00000       0.00000          1
L328      1.00000       1.00000      0.00000       0.00000          1
S213      1.00000       1.00000      0.00000       0.00000          1
S215      1.00000       1.00000      0.00000       0.00000          1
S221      1.00000       1.00000      0.00000       0.00000          1
S222      1.00000       2.00000      0.00000       0.00000          1
S237      1.00000       2.00000      0.00000       0.00000          1
D221      1.00000       1.00000      0.00000       0.00000          1
D222      1.00000       2.00000      0.00000       0.00000          1
D238      1.00000       1.00000      0.00000       0.00000          1
L216      1.00000       1.00000      0.00000       0.00000          1
S104      1.00000       1.00000      0.00000       0.00000          1
S118      1.00000       2.00000      0.00000       0.00000          1
BR02      1.00000       1.00000      0.00000       0.00000          1
D116      1.00000       1.00000      0.00000       0.00000          1


           TIME DURATION OF EACH OCCUPATION BY ADVERSARIES OVER RUNS
        --------------------------------------------------------------
NODE               STANDARD    STD. DEV.                        NUMBER
LABEL    MEAN      DEVIATION    OF MEAN      MINIMUM     MAXIMUM  OBS.
----------------------------------------------------------------------

S501   0.03000     0.00000     0.00000     0.03000     0.03000       2
S502   3.50000     0.00000     0.00000     3.50000     3.50000       1
D501   0.03000     0.00000     0.00000     0.03000     0.03000       2
L541   0.49000     0.50912     0.25456     0.13000     0.85000       2
S401   0.06500     0.04950     0.02475     0.03000     0.10000       2
L431   0.49000     0.50912     0.25456     0.13000     0.85000       2
S301   0.23373     0.02300     0.01150     0.21747     0.25000       2
S302   0.08000     0.00000     0.00000     0.08000     0.08000       1
S303   0.03000     0.00000     0.00000     0.03000     0.03000       1
D301   0.03000     0.00000     0.00000     0.03000     0.03000       1
D302   0.03000     0.00000     0.00000     0.03000     0.03000       1
L328   0.13000     0.00000     0.00000     0.13000     0.13000       1
S213   0.07000     0.00000     0.00000     0.07000     0.07000       1
S215   0.07000     0.00000     0.00000     0.07000     0.07000       1
S221   0.05000     0.00000     0.00000     0.05000     0.05000       1
S222   0.02500     0.00707     0.00354     0.02000     0.03000       2
S237   0.02000     0.01414     0.00707     0.01000     0.03000       2
D221   0.03000     0.00000     0.00000     0.03000     0.03000       1
D222   0.02500     0.00707     0.00354     0.02000     0.03000       2
D238   0.05000     0.00000     0.00000     0.05000     0.05000       1
L216   0.15000     0.00000     0.00000     0.15000     0.15000       1
S104   0.25000     0.00000     0.00000     0.25000     0.25000       1
S118   0.10000     0.00000     0.00000     0.10000     0.10000       2
BR02   0.00000     0.00000     0.00000     0.00000     0.00000       1
D116   0.02000     0.00000     0.00000     0.02000     0.02000       1
```

FIGURE 3-6 NODE STATISTICS

REFERENCES

3-1) Chapman, L.D., and Engi, D.,"Safeguards Network Analysis Procedure (Snap)-Overview," NUREG/CR-0960, SAND79-0438, Sandia Laboratories, August 1979.

3-2) Grant III, F. H., Minor, R.J., Chapman, L.D., and Engi, D., "Safeguards Network Analysis Procedure (SNAP)," NUREG/CR-0725, SAND79-0617, Sandia Laboratories, March 1979.

3-3) Grant III, F.H., Engi, D., and Chapman, L.D.,"User's Guide for SNAP," NUREG/CR-1245, SAND80-0315, Sandia National Laboratories, January 1981. (Except for some differences in authorship, and the inclusion of appendices describing advanced SNAP capabilities and SNAP error messages, this is nearly identical to the November 1978 Pritsker User's Guide.)

3-4) Grant III, F.H., Miner, R.J., and Engi, D.,"A Network Modeling and Analysis Technique for the Evaluation of Nuclear Safeguards Effectiveness," SAND78-0671, Sandia Laboratories, December 1978.

3-5) Miner, R.J., and Grant III, F.H.,"User's Guide for SNAP," Pritsker and Associates, Inc., November 1978.

3-6) Engi,D., and Chapman,L.D.,"Fixed Site Neutralization Model Programmer's Manual," Vol.1, Sandia Laboratories, SAND79-2242, December 1979.

CHAPTER 4

MAIT

INTRODUCTION

The other methodologies contained in this report address the problem of evaluating a physical security system against an overt threat. The problem consists of such factors as detection, confrontation, and denial including all the subdivisions of these categories such as communication, small combat modeling, optimal path generation, event time vs. success prediction, and final outcome determination.

One large problem area that such analyses are poorly equipped to address is the insider problem. Although this is discussed more thoroughly below, the insider or covert threat is quite different from the outsider or overt threat and must be dealt with accordingly. The main distinction between the two, aside from the fact that the insider has a much greater knowledge of the physical layout and operation of the ship, is that the insider has authorized access and control over much of the exterior and interior of the ship. Thus what constitutes formidable safeguards to the outsider, such as boarding passes, locked doors, motion detectors, etc. are merely part of the everyday working environment to the insider.

When one considers the special conditions that the shipboard scenario imposes on the physical security problem such as complicated and compartmented physical plans, numerous personnel categories, and multiple ship operating conditions, the potential threat of the insider becomes evident. Likewise, many of these same conditions impose psychological burdens on crew members which may lead to disaffection and alienation. Thus, authorization of access and control to the wrong person at the wrong time under the wrong condition may pose a more serious threat to the ship's security than the worst-case physical confrontation that could be generated by a group of outsiders.

The insider threat, although long recognized, had not been specifically addressed as a separate entity until more recently. In 1977, Science Applications, Inc. (SAI) began development of a digital computer oriented methodology designed to analyze the insider problem exclusively. Given the name MAIT (Matrix Analysis of the Insider Threat), this program has undergone an evolvement process which includes various applications and consequential upgrading. It is a derivative of this program that constitutes the basis of the SNWS analysis of the insider threat.

The original funding for the development of MAIT was provided by the Nuclear Regulatory Commission to analyze fixed-site nuclear facilities. Subsequent use of the program has been made by the Department of Energy, Department of Defense, and various private concerns. The program, although continually being modified and expanded, has been thoroughly tested and proven and today is an integral part of the security analysis procedures for Federal licensing of nuclear facilities.

A definite attempt has been made to present the mechanics of computation within a framework of the overall problem to be solved. Pursuant to this end, the next section is devoted to an in-depth discussion of the insider problem followed by a summary of the computer program itself. The emphasis in this section is on what is done rather than how it is done in order to avoid unnecessary detail. If the reader so desires, the bibliography at the end of the Chapter contains references that cover the spectrum from user's manuals to algorithm description. The next section discusses the current operational status of MAIT for the SNWS program at NSWC. The mechanics of running the program as well as some of the newer features that have been added to further enhance the analysis of the SNWS problem in particular are also included. Lastly, a listing of some of the highlights of the program is presented. Although some of these items are discussed in more depth elsewhere, this tabulation provides a quick summary of the MAIT methodology.

PROBLEM ADDRESSED

STATEMENT OF THE PROBLEM. The MAIT program analyzes the insider threat to shipboard nuclear weapons systems. Such threats include both theft and sabotage. The distinction between insider and outsider is det*rmined by authorization; the insider has authorized access and/oı control over specific physical safeguards whereas the outsider has no such advantage. The vulnerability of the safeguard system is determined by generating all possible paths from some given starting point to the target and, in the case of theft, to an additional location representing the exit point. Next, a vector is formed of all the safeguards along each path. These safeguards are then examined to see which are operational for the condition and threat currently being examined and are negated accordingly. A determination is made of the remaining safeguards to see which people aboard the ship have authorized access or control over them. In order to make the analysis as complete as possible, personnel can be considered to be working alone or in pairs where different delegated authority granted to each results in a higher internal threat capability. Thus the program provides such information as the most vulnerable paths to and from the target, which combinations of personnel can defeat the most safeguards along each path, how many safeguards remain on each path, and which safeguards are defeated most often by internal personnel.

BACKGROUND AND NATURE OF SOLUTION. As noted in Chapter 1, most modeling efforts address the safeguards problem as a physical confrontation. One prominant area that simulations of this type do not adapt well to is the insider problem. This is of particular concern to the Navy since ships are inherently encumbered with such features as concentration of people, many personnel categories, complicated and compartmented physical layouts, and numerous ship operating modes.

The MAIT simulation is currently the only program designed exclusively for examining the insider problem. The term "insider" is rather vague and should be better defined in context of the MAIT program in order to understand the specific problem addressed. First, it should be recognized that an overt physical attack on a guard or upon a security device by a crewmember is really not an insider problem but rather a subset of the outsider problem. The only variations in the two scenarios are: 1) the starting point may be within a perimeter that is closer to the target ("closer" connotes fewer safeguards), and 2) the adversary may have more detailed information concerning the layout of the ship, the nature of the safeguards, the operational status of the ship, etc.

The primary distinction made by MAIT between insider and outsider is that the former has authorized access and/or control over one or more safeguards protecting the potential target. Access is defined by SAI as "1) the safeguard is not applied to the individual or pair, or 2) the safeguard is applied to the individual or pair but the alarm is ignored" (ref. 4-5). Similiarly control is defined "to mean either direct control of a safeguard or device or indirect control which may be exercised by ignoring alarms, tampering, or directing others to ignore alarms or bypass certain personnel" (ref. 4-5).

Particular emphasis of the word "authorized" should be made in the above definitions as this is the underlying basis of the entire MAIT program. If a person has authorized access or control over a safeguard, the need to resort to coercion, deception, or physical force is negated. Thus the MAIT analysis provides an assessment of the insider threat before such adversaries assume capabilities that are equally assignable to outsiders as well. Once the true insider situation is ascertained, then the safeguards can be reassessed to decide what additional capabilities in terms of coercion, deception, and force are needed, if any, to compromise the entire system.

There are several subtle but important implications arising from the fact that we are concerned with authorized insiders as opposed to force-oriented outsiders. The first of these is that space and distance have no meaning other than providing a framework within which the safeguards are located. As an example, an adversary path is not measured in distance but rather in the number of safeguards encountered. Thus a path which includes many decks, gangways, compartments, stairways, etc. is considered easily traversable by an authorized person compared to passage through a single portal for which the same person is not authorized.

Time, usually the independent variable in most physical security analyses, is almost irrelevant in the MAIT program. An insider either has or does not have access or control over a given safeguard. The important exception to this concept is that the authorization granted an insider may change when there is a change of condition in the ship's operational status. An example would be that a person could not exit through a certain locked door under normal operating conditions but this door may be automatically unlocked during emergency conditions. It is very likely that a knowledgeable insider planning an act of sabotage or theft would take advantage of any such variation in his authority. Thus, the MAIT program has provision for analyzing the consequences of change of condition.

A final point arising from the unique nature of the insider is the binary nature of the problem. An insider, for any given threat and condition, either has or does not have access or control to elements of the security system. Thus there is no probability distributions associated with an event happening or not. Likewise data such as how long it will take to defeat a lock and its ancillary of how the probability of detection varies with time is again irrelevant; the insider either has authorization to open the lock or he doesn't.

As mentioned above, the MAIT program does not restrict the adversary to one person. The determining factor in categorizing the crew of a ship, any of which is a potential adversary, is again based upon authorization. Thus if a complement of 50 weapons specialists all had the same authority over specific safeguards, they would be considered as one person of a person-pair combination. This is because all 50, or any combination thereof, have no more or no less capability over safeguards than any one individual within the same group. Conversely, any other crew member who has any other authorization for any threat under any condition would have to be considered as another personnel category. By being able to analyze two such categories working together the performance of the program is greatly increased. As an example, the threat consisting of a "runner" working with a guard who is monitoring an alarm can be examined by MAIT. In summary, MAIT is designed to handle person-pair combinations where either of the pair may range in number from zero (to handle the single person threat) to the total number of personnel within any given category.

This section has been included to introduce the reader to the overall insider problem addressed by MAIT and to summarize the methodology used to analyze this type of threat. A more thorough discussion of the program attributes are included in the following sections.

DESCRIPTION OF THE PROGRAM

INTRODUCTION. The purpose of this section is to present a brief, non-technical description of the computational mechanics of the program. However, this description is meaningful only if presented in the framework of the entire insider problem discussed above. Therefore the following section presents the overall approach used in the MAIT analysis of which only a portion is the actual computer program. After this overview, a description of the program itself is presented including what is calculated and how it is done. The final two sections discuss the input data requirements and the types of information that are generated by the program.

THE MAIT METHOD. The MAIT method consists of essentially three steps that are iterated until some acceptance level is reached. This process is summarily shown in Figure 4-1. The three steps are: 1) facility modeling, 2) MAIT computer analysis, and 3) assessment. These steps are discussed below with the aim of presenting the computer program in context of the overall problem as mentioned above.

Acceptance Criteria. Acceptance criteria must be established first in order to determine what upgrading of the physical security system needs to be done, how quickly this level is being reached, and when the iteration process can be terminated. The acceptance criteria will vary from ship to ship but is likely to be composed of factors such as total number of paths from the starting point to the target, the number of safeguards remaining after applying the access and control capabilities for every person-pair combination for each threat and condition, safeguards most easily defeated, etc. As with any complex problem, an element of judgment must be exercised in place of reliance on an arbitrary set of numbers. As an example, the fact that the Captain and the Nuclear Weapons Officer combination have access and/or control authority over most safeguards may have to be deemed acceptable in the practical situation of operating a ship although the analysis rates this as a severe security problem.

Data Collection And Facility Modeling. Before a computer can used to determine the level of security afforded by a safeguards system, the ship must be completely modeled in terms of the location of its safeguards, the threat and conditions for which they are operable, and which of the crew have access or control over these safeguards. Indeed, the very act of systematically collecting the necessary data has proven to be a very valuable exercise in itself for assessing the safeguards system. The complete safeguard structure can be described by six two-dimensional binary matrices which are discussed below.

The first step is to map the multi-level ship in terms of a 2-dimensional location adjacency matrix. The location matrix has "location" as the dimension in both directions and relates if and how travel can be accomplished from one location to another. This matrix is used to generate the paths form the initial point to the target, and in the case of theft, to another point on the perimeter of the safeguard system. The 2nd of the six matrices is the safeguards matrix which has "location-safeguards" as the two dimensions and obviously merely maps the location of the safeguards. The 3rd and 4th matrices establish the operational status of each safeguard. The first maps threat (sabotage, theft, etc.) as a function of safeguards and is dimensioned "threats-safeguards" while the second relates operational status of the ship (normal cruise, dock, emergency, etc.) and is dimensioned "conditions-safeguard". The final two matrices, the 5th and 6th, contain the access and control capabilities of every person-pair over every safeguard and have the dimensions of "access-safeguards" and "control-safeguards" respectively.

A point that needs restressing is the systematic nature that is inherent in the data collection process for MAIT. Initially all safeguards aboard the ship need to be identified and a location adjacency map of the ship must be generated on which a unique position for every safeguard can be mapped. Then the threats, conditions, and personnel categories must be identified and listed. Once these tasks are accomplished, the analyst, usually with the help of large, 2-dimensional tables, merely has to ascertain which safeguards are applicable for which person-pairs under which conditions. In summary, the emphasis must be on completeness since the omission of a single personnel category or a single safeguard can greatly reduce the validity of the results. As with all of the models, the very act of completing the tables containing the input data has provided a valuable insight into the effectiveness of the security system even before any computer analysis has been generated.

Mait Computer Analysis. This section briefly describes the order of calculation performed by the computer without getting involved in detail. The description is presented in terms of what data is now available at this stage of calculation and how the results of the current calculation are leading closer to the desired solution. For those interested in a more detailed description of the entire program, a bibliography is included at the end of the Chapter which references reports that contain this type of information.

As described above, we enter the computerized portion of the analysis with six two-dimensional binary matrices that model the entire physical security system of the ship. The calculation process can be summarized in three steps: 1) determine the path which the insider adversary will make from his designated starting point to the target; form a vector of the safeguards found along this path, 2) condition the safeguards vector for both threat and condition, and 3) condition the safeguards vector for the authorized access and control capabilities of each person-pair. The result of these operations is a vector of safeguards, if any are left, along the given path that have not been negated by one or more of the factors above.

In summary, the MAIT program performs a commonality analysis to determine what safeguards remain in effect along a given path after the capabilities of authorized access and control of one or two personnel categories are applied. This process is repeated for every possible path from the start to the target as designated by the analyst, for every person-pair combination, and for every threat and ship operational condition. Since a person either has access and/or control over a safeguard or he doesn't, all the inputted data and numerical manipulation is binary in nature. The results of the program yield information concerning each safeguard, each person-pair combination, each threat, and each operational condition. This yields not only an evaluation of the current overall security system but provides an insight into how the system can be best upgraded as discussed in the following section.

Assessment. The primary purpose of the MAIT approach is not only to evaluate the security system as it now stands but determine how the system can be upgraded in the most optimal manner. In order to do this, the analyst needs to have available information such as the paths most likely taken, under what conditions would an insider most likely try to compromise the security system, what person or pair of persons present the greatest threat for sabotage or theft, what safeguards are most easily defeated, etc. To provide this kind of data, the MAIT program has 2 computational characteristics that are absolutely essential in this kind of analysis: 1) it is exhaustive; every combination of path, condition, threat, and person-pair is examined, 2) the data is kept segregated according to these same parameters so that each may be examined in the light of the others.

Before discussing the output data, two terms need defining. An "event" is one combination cf the factors that are permuted, these being path, person-pair, threat, and condition. In order to limit the output arising from these combinations, the analyst may set a criticality level which determines the number of safeguards remaining on the path for any one event. Thus if two is selected as the critical number, the only data retained is those events with two or less safeguards remaining on the path after threat, condition, access, and control are applied. The analyst will usually start with a criticality level of 0 which lists only those events where all the safeguards have been defeated. As the security system is upgraded, the criticality number can be raised accordingly and yet keep the data output within bounds.

A sample of the output data is shown on Figures 4-6. Rather than laboriously discuss this output line by line, the highlights may be tabulated as follows:

(1) The input data is echoed to the output device as a check for later review.

(2) The six binary matrices are presented in an abbreviated form to allow the analyst to make sure the physical facility is modeled correctly and the problem being addressed is the problem desired.

(3) The path written is comprised of a series of location numbers; every path is printed and all information listed below is provided with each path.

(4) All the safeguards along the path are printed.

(5) The safeguards that are negated because they do not apply to the current threat are output; the remaining safeguards are printed.

(6) The safeguards that are negated because they do not apply to the current ship operational condition are output; the remaining safeguards are printed.

(7) The location and name of each safeguard remaining on the path after calculation of 6) above is provided along with the person-pair combination that can negate the safeguard either by access or control.

(8) Summary information that combines the results of the entire analysis is provided including:

(a) Total number of paths generated.

(b) Number of critical events.

(c) Number of events with 0,1,2,...12 safeguards remaining; these numbers as a percent of the total events.

(d) Safeguards defeated most often.

(e) Person-pairs that appear most often in critical paths.

(f) Conditions under which critical events occur most often.

Note in the above description that there are two basic types of output given by the MAIT program: 1) detailed output for each event, and 2) summary output for the entire analysis. A postprocessor capability is provided with MAIT to perform the detailed analysis. This is essentially an ancillary program with which the analyst can probe the results of the main program more thoroughly. The postprocessor is an interactive program which allows the analyst to select from a computer terminal which path, threat, and condition he wants to examine. Thus, information such as how person-pair (4,7) defeated safeguard 28 on the 5th path is provided. The big advantage of setting up the program run architecture in this manner is that it eliminates the time consuming rerunning of the main program every time a new facet of the output must be reexamined. This ability is provided automatically for the user and is accomplished by storing all of the interim calculations to be accessed by the postprocessor at a later date.

The iterative refinement-analysis process must be continued until the acceptability criteria are met or the closest approach possible within the given constraints is reached. Even when the security system is deemed acceptable, MAIT still points out the weakest link in the security chain and shows where any additional upgrading of the system would result in the greatest improvement.

MAIT IMPLEMENTATION

This section discusses how MAIT is being implemented and used at NSWC on the SNWS program. The purpose of this discussion is to describe the current MAIT setup at NSWC and to point out some of the problem areas peculiar to the Naval insider problem.

PROGRAM RUN ARCHITECTURE. A schematic illustrating the sequence for executing a MAIT run on the INTERDATA 7/32 is shown on Figure 4-2. The following discussion references this diagram:

(1) Generate a new data file or edit a stored file.

The input for theft and/or sabotage version of MAIT is read directly by the program from a magnetic disk file; a text editor is available to make the creation of a new file or the modification of an existing file a relatively easy task; the current philosophy is to have a "standard" data file for each class of ships from which the file for a specific ship could readily be generated.

(2) Run the main program.

A simple input command from the console will cause execution of the main MAIT program; the parameters in this command designate: 1) the input data file to be used, 2) the names of the files to store the intermediate data generated by the main program for later use by the postprocessor, and 3) whether the output generated is to be displayed on the console or the printer.

(3) Run the postprocessor.

The input command stream entered from the console designates the magnetic files to be used and whether the output goes to the console or to the printer; the user must also enter four parameters from the console (threat, condition, and the person-pair); these four variables allow the analyst to determine how specific safeguards are defeated along a specific path.

CURRENT OPERATIONAL STATUS. This discussion of the status of MAIT at NSWC is broken into two subtopics: 1) the status of the code itself, and 2) how the overall MAIT methodology is being implemented.

When first written in 1977, the MAIT program was designed for analysis of fixed-site nuclear processing plants. Although the program was readily adaptable to the Navy insider problem, several areas needed strengthening for optimal long-term usage. A joint effort by SAI and NSWC has produced numerous upgrades with the more important being enumerated as follows:

(1) Improvements in the program's numerics and logic to produce faster run times.

(2) Formatting changes to make the output more readable and more oriented to the SNWS problem.

(3) The addition of path counters and limiters to initially size the problem.

(4) Implementation of a location translator which permits the analyst to identify locations on the ship by any numbering system he choses; this feature allows MAIT to use the same numerical locations as may be present on the blueprints or which may be used by other programs analyzing the ship's safeguards system; an extension of this feature would be the use of a common data base among all the computer programs.

(5) Secondary targets on all paths are now provided for; this is a realistic improvement in that many scenarios call for the adversary to first obtain a key or to perform some other similar initial action prior to the main approach to the target.

(6) The program was originally divided into two distinct codes for theft and sabotage threats; it has now been combined with a single input command designating which threat is to be analyzed.

(7) Change of ship operational condition is taken into consideration; this is perhaps the most important of the updates and has been discussed above.

One irreversible limitation of this approach that must be dealt with is that almost every ship within a class will vary from the baseline case in either physical layout, composition of crew, work rules, or safeguards present. Since time limitations prohibit the analysis of every ship within the group, any proposed modification must be acceptable on a class basis without compromising the effectiveness of the proposed change.

The data collection process for the MAIT effort on the SNWS program has provided a great deal of insight into the effectiveness of both the current safeguards system and the overall physical security measures currently being implemented. The physical layouts for the ship classes is derived mostly from engineering drawings and is supplemented by ship visitations. A more difficult task is obtaining the data pertaining to who has access or control over particular safeguards. Most of this data is extracted from the shipboard security plans but these have proven to lack uniformity from ship to ship and to be very incomplete. Fleet personnnel have often been the best source of this information although deciphering the administrative procedures to obtain sensitive data is a time-consuming task.

The main problem so far in implementing MAIT for the SNWS program has been the classification of personnel aboard ships according to their authorized access and control attributes. The analysts have found that many "gray" areas exist in this classification process and a great deal of time must be spent to understand the true situation so that arbitrary decisions are not made. On the other hand, the MAIT program has been found very easy to run.

In summary, the MAIT program has proven a valuable tool in the analysis of the insider problem pertaining to the naval physical security system. With the inclusion of the above features, the program has been deemed satisfactory and proven from a computational standpoint.

COMPUTATIONAL REQUIREMENTS. The following presents a list of computational requirements that are needed to make a typical MAIT run at NSWC:

(1) Run time: typical problem involving approximatly 100 paths with 50 locations runs in about 200 seconds; this varies with the specific problem involved.

(2) Core and 250 KB MAIT program; disk:2 MB MAIT user disk space.

(3) Source code in FORTRAN; readily adaptable to other and miscellaneous computers with changes in input-output commands and logic masking functions possibly needed.

SAMPLE PROBLEM. This sample problem was developed during a tutorial course conducted by T. M. McDaniel of SAI on the use of the MAIT program. It is nonclassified since it does not refer to any ship in particular and is included here merely for illustrative purposes. For a full discussion of the problem, the reader is referred to the SAI user's manual (ref. 4-5).

Figure 4-3 presents the physical layout of the area to be analyzed; note that it is a 3-dimensional "unfold" diagram which shows spatial interrelationships but is not meaningful as a schematic. The locations, threats, conditions, personnel categories, and safeguards are listed on Figures 4-4 and 4-5.

Only the first iteration of the analysis is presented. The complete summary output is included to illustrate the "playback" and "dump" options as well as each critical path vector and its conditioning by threat and operational condition. Note that the relationship between the safeguards and location, threat, conditon, access and control are given on Figure 4-6. The summary results on Figure 4-6 show the initial security system to be very porous with 288 (or 25%) of the total number of events to have zero safeguards remaining. It can also be seen that P9, the Nuclear Weapon Security Force, comprise a large proportion of the critical events. Also, it should be noted that 54% of the critical events occur during the At Sea Normal condition (C4) while 21% occur under condition C5.

With these results in hand, the analyst can now begin the iterative process of modifying the parameters of access, control, location, and workrules to upgrade the system in the most optimum manner. As mentioned before, this is not a simple task in that solutions that look good on paper may be completely unworkable from an operational or cost standpoint. Sometimes a simple change that is not obvious proves to be more effective than several alternatives that on the surface seem more promising. The cross-referencing of the above parameters by MAIT with all the remaining parameters help a well-trained analyst guard against this difficulty. Although not presented here, five additional iterations including the basis for the changes from one to another as well as their effects on the entire safeguards system are presented in another report (ref. 4-7).

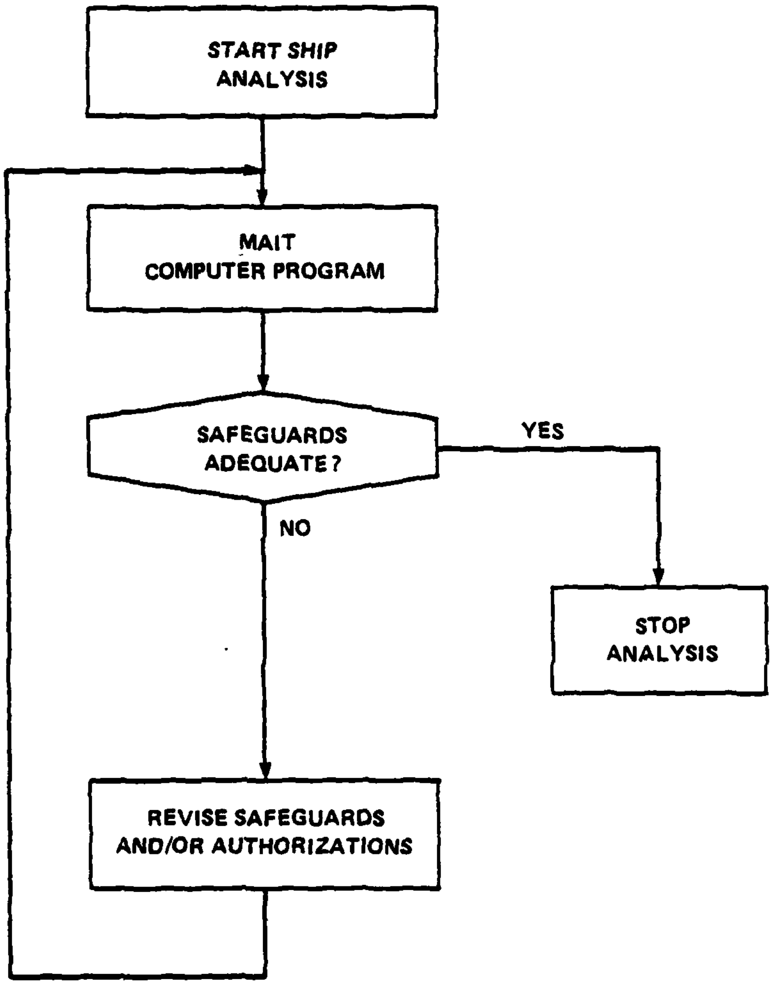


FIGURE 4-1 MAIT METHODOLOGY

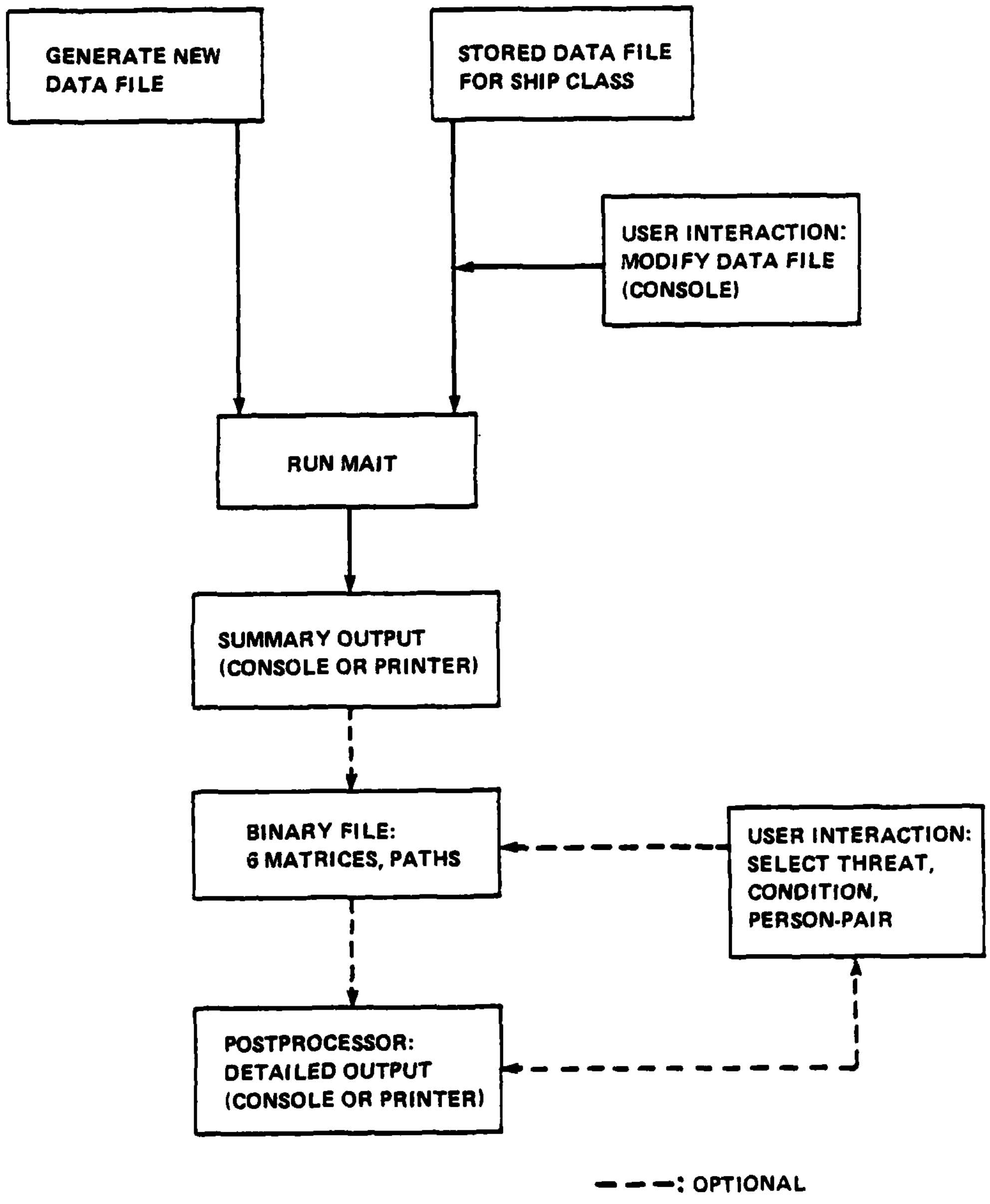

GENERATE NEW DATA FILE
STORED DATA FILE FOR SHIP CLASS
USER INTERACTION: MODIFY DATA FILE (CONSOLE)
RUN MAIT
SUMMARY OUTPUT (CONSOLE OR PRINTER)
BINARY FILE: 6 MATRICES, PATHS
USER INTERACTION: SELECT THREAT, CONDITION, PERSON-PAIR
POSTPROCESSOR: DETAILED OUTPUT (CONSOLE OR PRINTER)
– – –: OPTIONAL

FIGURE 4-2 PROGRAM RUN ARCHITECTURE

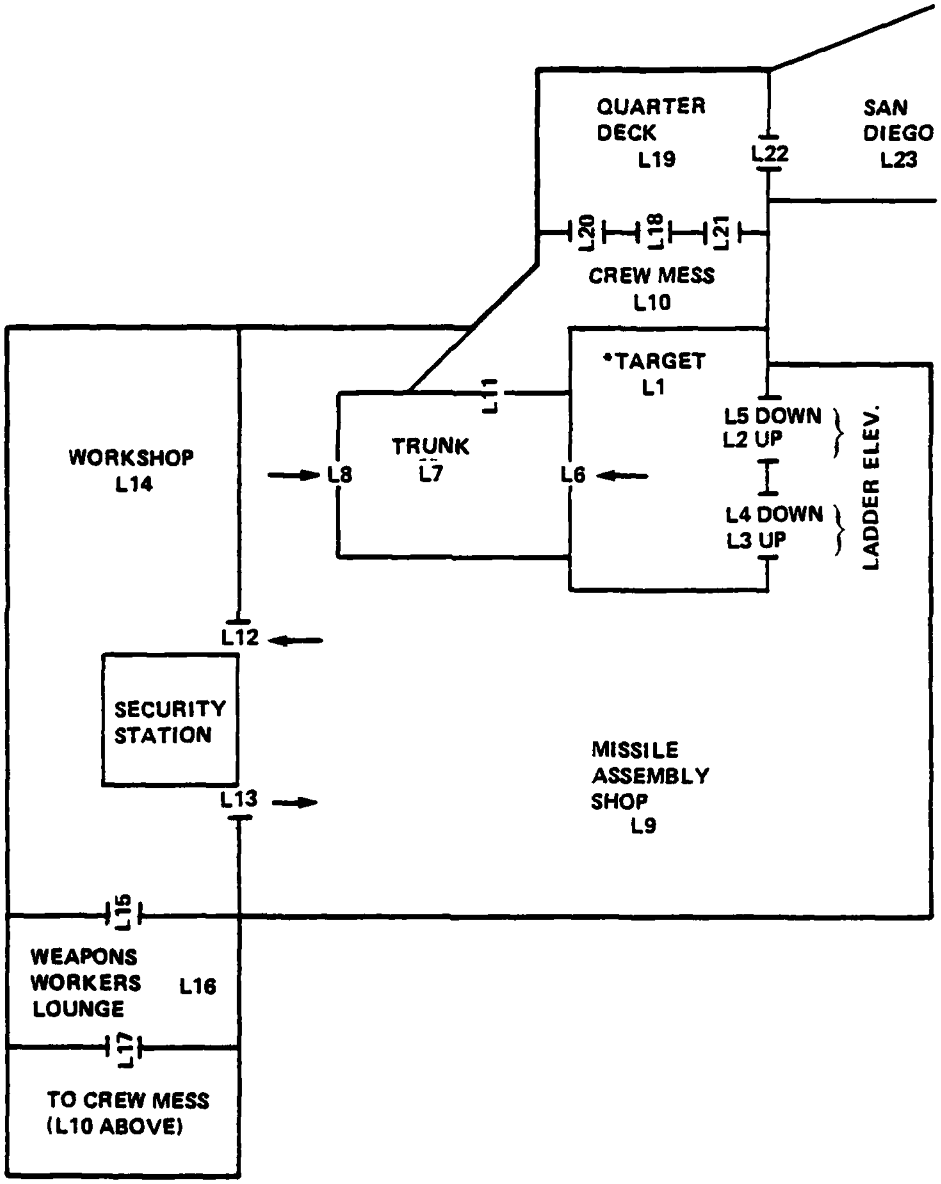


FIGURE 4-3 SAMPLE PROBLEM LAYOUT

Locations

L1	target (magazine)
L2	elevator up door; between L1 and L9
L3	ladder up door; between L1 and L9
L4	ladder down door; between L1 and L9
L5	elevator down door; between L1 and L9
L6	doorway (one way); from L1 to L7
L7	trunk
L8	doorway (one way); from L9 to L7
L9	missile assembly shop
L10	crew mess
L11	passageway; between L10 and L7
L12	doorway (out); from L9 to L14
L13	doorway (in); from L14 to L9
L14	workshop
L15	doorway; between L14 and L16
L16	weapons workers lounge
L17	passageway; between L16 and L10
L18	passageway; between L10 and L19
L19	quarterdeck
L20	passageway; between L19 and L10
L21	passageway; between L19 and L10
L22	passageway; between L19 and L23
L23	rest of world

Threats

T1	theft in
T2	theft out
T3	sabotage (used in this example)

FIGURE 4-4 SAMPLE PROBLEM PARAMETERS

Conditions

C1	deck shift #1
C2	deck shift #2
C3	deck shift #3
C4	at sea normal
C5	no access to L13 (door locked)

Personnel

P1	Commanding Officer
P2	Nuclear Weapons Officer
P3	Weapons Officer (conventional)
P4	security force (security station)
P5	weapons crew (maintenance of weapons)
P6	electronic technician
P7	general maintenance
P8	other crew and visitors
P9	nuclear weapons security force

Safeguards

S1	ID check (for boarding); L22
S2	item check (for boarding); L22
S3	ID check at security station; L13
S4	door locks; L13, L3, L4, L2, L5
S5	door alarms; L3, L4, L2, L5, L6, L8, L12, L13
S6	door pins (inside); L6, L8, L12

FIGURE 4-4 SAMPLE PROBLEM PARAMETERS (CONTINUED)

```
MATRIX     YSIS AGAINST THREATS INVOLVING INSIDER COLLUSION (MA     - VERSION 1. - SABOTAGE

*TIT  CLASS TEST PROBLEM 1
*RLOC L23/SAN DIEGO/,L22/GANGWAY/,L19/QUARTERDECK/.
L19,L21,L10/MESS/.
L19,L18,L10.
L19,L20/HATCH #2/L10.
L10,L11/TRUNK DOOR/,L7/TRUNK/.
L10,L17/STAIRWAYS/,L16/WAW LOUNGE/.
L16,L15/WORKSHOP DOOR/,L14/WORKSHOP/.
*LOC  L1/TARGET/,L6/TRUNK DOOR/,L7.
L9/4AS/,L8/TRUNK DOOR/,L7.
L9,L12/WTHSL-1/,L14.
L14,L13/WTHSL-2/,L9.
L9,L5/EL DOWN/,L1.
L1,L2/EL UP/,L9.
L1,L3/LADDER UP/,L9.
L9,L4/LADDER DOWN/,L1.
*SAF  S1/ID OR SEC CHK/,L22,PC4/SECURITY FORCE/,PA1/C.O./,
PA2/W.W.OFFICER/,PA3/WEAPONS OFF/,PA4,PA5/WEAPONS CREW/,PA6/ET/,
PA7/GEN. MAINT./,PA8/OTHER CREW CVIS./,PA9/NUC.WEAP.SEC./,
T3/SABOTAGE/,C1/DECK SHIFT 1/,C2/DECK SHIFT 2/,C3/DECK SHIFT 3/.
S2/ITEM CHECK IN/L22,PC4,C1,C2,C3,T3.
S3/ID CHECK/,L12,L13,PC9,PA(1,2),PA(1,3),PA(1,4),PA(1,5),PA(1,8),
PA(1,9),PA(2,3),PA(2,4),PA(2,5),PA(2,6),PA(2,7),PA(2,8),
PA(3,4),PA(3,5),PA(3,6),PA(3,7),PA(3,8),PA(3,9),PA(5,5),
PA(9,9),T3,C1,C2,C3,C4/AT SEA NORM./.
S4/L)CK/L2,L3,L4,L5,L13,PC1,PA1,PA(1,2),PA(2,3),PA(1,3),T3,C5.
S5/ALARM/,L2,L3,L4,L5,L8,L6,L12,L13,PC1,PC2,PC3,PC4,T3,C5/NO ACCESS/.
S6/PIN LOCK/,L6,L12,L8,PC(2,9),PC(5,5),PC(2,3),PC(2,5),T3,C5.
*DUM
*PLA S.

• • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • •
```

FIGURE 4-5 SAMPLE PROBLEM INPUT

```
PLAYBACK

    LOCATION        ADJ    SAFEGUARD          PERS. ACCESS          PERS. CONTROL       THREAT          CONDITION

 22 GANGWAY          19    1 ID OR SEC CHK    1 C.O.                4 SECURITY FORCE    3 SABOTAGE      1 DECK SHIFT 1
                     23                       2 N.W.OFFICER                                             2 DECK SHIFT 2
                                              3 WEAPONS OFF                                             3 DECK SHIFT 3
                                              4 SECURITY FORCE
                                              5 WEAPONS CREW
                                              6 FT
                                              7 GEN. MAINT.
                                              8 OTHER CREW SVIS.
                                              9 NUC.WEAP.SEC.

 22 GANGWAY          19    2 ITEM CHECK IN                          4 SECURITY FORCE    3 SABOTAGE      1 DECK SHIFT 1
                     23                                                                                 2 DECK SHIFT 2
                                                                                                        3 DECK SHIFT 3

 12 WTHSL-1          14    3 ID CHECK           ( 1,  2)            9 NUC.WEAP.SEC.     3 SABOTAGE      1 DECK SHIFT 1
 13 WTHSL-2           9                         ( 1,  3)                                                2 DECK SHIFT 2
                                                ( 1,  4)                                                3 DECK SHIFT 3
                                                ( 1,  5)                                                4 AT SEA NORM.
                                                ( 1,  9)
                                                ( 1,  9)
                                                ( 2,  3)
                                                ( 2,  4)
                                                ( 2,  5)
                                                ( 2,  6)
                                                ( 2,  7)
                                                ( 2,  8)
                                                ( 3,  4)
                                                ( 3,  5)
                                                ( 3,  6)
                                                ( 3,  7)
                                                ( 3,  9)
                                                ( 3,  9)
                                                ( 5,  5)
                                                ( 9,  9)

  2 EL UP             9    4 LOCK             1 C.O.                1 C.O.              3 SABOTAGE      5 NO ACCESS
  3 LADDER UP         9                         ( 1,  2)
  4 LADDER DOWN       1                         ( 1,  3)
  5 EL DOWN           1                         ( 2,  3)
 13 WTHSL-2           9

  2 EL UP             9    5 ALARM                                  1 C.O.              3 SABOTAGE      5 NO ACCESS
  3 LADDER UP         9                                             2 N.W.OFFICER
  4 LADDER DOWN       1                                             3 WEAPONS OFF
  5 EL DOWN           1                                             4 SECURITY FORCE
  6 TRUNK DOOR        7
  9 TRUNK DOOR        7
 12 WTHSL-1          14
 13 WTHSL-2           9

  5 TRUNK DOOR        7    6 PIN LOCK                                 ( 2,  3)          3 SABOTAGE      5 NO ACCESS
  8 TRUNK DOOR        7                                               ( 2,  5)
 12 WTHSL-1          14                                               ( 2,  9)
                                                                      ( 5,  5)
```

FIGURE 4-6 SAMPLE PROBLEM OUTPUT

```
FACILITY DUM      CLASS TEST PROBLEM 1

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

LOCATION ADJACENCY MATRIX

  1  TARGET
  2  EL UP
  3  LADDER UP
  4  LADDER DOWN
  5  EL DOWN
  6  TRUNK DOOR
  7  TRUNK
  8  TRUNK DOOR
  9  MAS
 10  MESS
 11  TRUNK DOOR
 12  WTMSL-1
 13  WTMSL-2
 14  WORKSHOP
 15  WORKSHOP DOOR
 16  MAW LOUNGE
 17  STAIRWAYS
 18  UNDEFINED
 19  QUARTERDECK
 20  HATCH #2
 21  UNDEFINED
 22  GANGWAY
 23  SAN DIEGO

                 1         2
    1 1**45*78901234567890123
    2 12345678*01234567890123
    3 12345578*01234567890123
    4 *2345678901234567890123
    5 *2345678901234567890123
    6 123456*8901234567890123
    7 1234557890*234567890123
    8 12345**890*234567890123
    9 123*567*9[illegible]34567890123
   10 1234567890*23456**9**23
   11 123456*89*1234567890123
   12 1234567890123*567890123
   13 12345678*01234567890123
   14 123456789012*4*67890123
   15 1234557890123*5*7890123
   15 12345578901234*6*890123
   17 123456789*12345*7890123
   18 123456789*12345678*0123
   19 12345678901234557*9**23
   20 123456789*12345678*0123
   21 123456789*12345678*0123
   22 123456799012345678*012*
   23 123456799012345678901*3
```

FIGURE 4-6 SAMPLE PROBLEM OUTPUT (CONTINUED)

```
SAFEGUARD BY LOCATION

 1  ID OR SEC CHK
 2  ITEM CHECK IN
 3  ID CHECK
 4  LOCK
 5  ALARM
 6  PIN LOCK
                 1         2
   1 123456789012345678901*3
   2 123456789012345678901*3
   3 12345678901**4567890123
   4 1****6789012*4567890123
   5 1*****7*901**4567890123
   6 12345*7*901*34567890123
PERSONNEL ACCESS BY SAFEGUARD

 1  C.O.
 2  N.W.OFFICER
 3  WEAPONS OFF
 4  SECURITY FORCE
 5  WEAPONS CREW
 6  ET
 7  GEN. MAINT.
 8  OTHER CREW EVIS.
 9  NUC.WEAP.SEC.

    1 *23*56
    2 *23456
    3 *23456
    4 *23456
    5 *23456
    6 *23456
    7 *23456
    8 *23456
    9 *23456
 1, 2 12**56
 1, 3 12**56
 1, 4 12*456
 1, 5 12*456
 1, 8 12*456
 1, 9 12*456
 2, 3 12**56
 2, 4 12*456
 2, 5 12*456
 2, 6 12*456
 2, 7 12*456
 2, 8 12*456
 3, 4 12*456
 3, 5 12*456
 3, 6 12*456
 3, 7 12*456
 3, 8 12*456
 3, 9 12*456
 5, 5 12*456
 [illegible] 12*456
```

FIGURE 4-6 SAMPLE PROBLEM OUTPUT (CONTINUED)

```
PERSONNEL CONTROL BY SAFESUARD


     1 123**6
     2 1234*6
     3 1234*6
     4 **34*6
     9 12*456
  2. 3 12345*
  2. 5 12345*
  2. 9 12345*
  5. 5 12345*



THREAT BY SAFEGUARD

  1  UNDEFINED
  2  UNDEFINED
  3  SABOTAGE

     3 ******



CONDITION BY SAFESUARD

  1  DECK SHIFT 1
  2  DECK SHIFT 2
  3  DECK SHIFT 3
  4  AT SEA NORM.
  5  NO ACCESS

     1 ***456
     2 ***456
     3 ***456
     4 12*456
     5 123***

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

FIGURE 4-6 SAMPLE PROBLEM OUTPUT (CONTINUED)

```
PATH VECTOR    23    22    19    18    10    17    16    15    14    13    9    4    1
                   1         2
  1 *23*5678**12*******01**

SAFESUARDS VECTOR

  1 *****5

SAFEGUARDS VECTOR:  THREAT 3

  1 *****6

SAFEGUARDS VECTOR:  THREAT 3  CONDITION 1

  1 ***456

SAFEGUARDS VECTOR:  THREAT 3  CONDITION 2

  1 ***456

SAFEGUARDS VECTOR:  THREAT 3  CONDITION 3

  1,***456

SAFEGUARDS VECTOR:  THREAT 3  CONDITION 4

  1 12*456

SAFEGUARDS VECTOR:  THREAT 3  CONDITION 5

  1 123**6

THREAT 3. NO. OF CRITICAL ENTRIES FOR THIS PATH =   48
PATH VECTOR    23    22    19    18    10    17    16    15    14    13    9    5    1
                   1         2
  1 *234*678**12*******01**

SAFEGUARDS VECTOR

  1 *****6

SAFEGUARDS VECTOR:  THREAT 3

  1 ***3*6

SAFEGUARDS VECTOR:  THREAT 3  CONDITION 1

  1 ***455

SAFEGUARDS VECTOR:  THREAT 3  CONDITION 2

  1 ***456

SAFEGUARDS VECTOR:  THREAT 3  CONDITION 3
```

FIGURE 4-6 SAMPLE PROBLEM OUTPUT (CONTINUED)

```
FACILITY SUMMARY     CLASS TEST PROBLEM 1

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

NUMBER/PERCENT OF EVENTS WITH N SAFEGUARDS REMAINING
   0     1     2
 288   606   252
25.1  52.9  22.0

CRITICAL LEVEL =  0, NUMBER CRITICAL =  288, PERCENT CRITICAL =  25.1

ID/NUMBER/PERCENT (OF CRITICAL) OF SAFEGUARDS DEFEATED MOST OFTEN (TOP 20) IN CRITICAL PATHS
   3     1     2     4     5     6     0     0     0     0     0     0     0     0     0     0     0     0     0     0
 228    72    72    60    60     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0
79.2  25.0  25.0  20.8  20.8    0.    0.    0.    0.    0.    0.    0.    0.    0.    0.    0.    0.    0.    0.    0.

UNDEFEATED SAFEGUARD ID/NO. OF EVENTS WITH ONE SAFEGUARD REMAINING
   2     4     3
 396   120    90

UNDEFEATED SAFEGUARD ID/NO. OF EVENTS WITH TWO SAFEGUARDS REMAINING
   2     3
 252   252

NUMBER/PERCENT OF CRITICAL EVENTS PER TARGET
  L  1/TARGET          /
            288
          100.0

NUMBER AND PERCENT OF CRITICAL EVENTS BY PERSON-PAIR
  PERSON-PAIR      NO. OF EVENTS      PERCENT OF TOTAL
      ( 1, 1)            6                  2.1
      ( 1, 2)           12                  4.2
      ( 1, 3)           12                  4.2
      ( 1, 4)           30                 10.4
      ( 1, 5)           12                  4.2
      ( 1, 6)            6                  2.1
      ( 1, 7)            6                  2.1
      ( 1, 8)           12                  4.2
      ( 1, 9)           12                  4.2
      ( 2, 3)           12                  4.2
      ( 2, 4)           24                  8.3
      ( 2, 5)            6                  2.1
      ( 2, 6)            6                  2.1
      ( 2, 7)            6                  2.1
      ( 2, 8)            6                  2.1
      ( 2, 9)            6                  2.1
      ( 3, 4)           24                  8.3
      ( 3, 5)            6                  2.1
      ( 3, 6)            6                  2.1
      ( 3, 7)            6                  2.1
      ( 3, 8)            6                  2.1
      ( 3, 9)            6                  2.1
      [illegible]       24                  [illegible]
```

FIGURE 4-6   SAMPLE PROBLEM OUTPUT (CONTINUED)

```
         ( [illegible])          6
         ( 6, 9)                 6              2.1
         (    3)                 6              2.1
         (    9)                 6              2.1
         ( 9, 9)                 5              2.1

NUMBER/PERCENT OF CRITICAL EVENTS PER THREAT
   T3/SABOTAGE        /
              288
            100.0

NUMBER/PERCENT OF CRITICAL EVENTS BY CONDITION
   C1/DECK SHIFT 1     /          C2/DECK SHIFT 2      /         C3/DECK SHIFT 3      /        C4/AT SEA NORM.      /        C5/NO ACCESS
               24                              24                             24                             156                              60
              8.3                             8.3                            8.3                            54.2                            20.8

NUMBER OF CRITICAL EVENTS BY PERSON-PAIR, BY THREAT AND CONDITION
      CONDITION     1/DECK SHIFT 1     /     2/DECK SHIFT 2     /     3/DECK SHIFT 3     /     4/AT SEA NORM.     /     5/NO ACCESS

3/SABOTAGE         /         ( 1, 4)  6             ( 1, 4)  6             ( 1, 4)  6             ( 1, 2)  6             ( 1, 1)  6
                             ( 2, 4)  5             ( 2, 4)  6             ( 2, 4)  6             ( 1, 3)  6             ( 1, 2)  6
                             ( 3, 4)  6             ( 3, 4)  6             ( 3, 4)  6             ( 1, 4)  6             ( 1, 3)  6
                             ( 4, 9)  5             ( 4, 9)  6             ( 4, 9)  5             ( 1, 5)  6             ( 1, 4)  6
                                                                                                  ( 1, 8)  6             ( 1, 5)  6
                                                                                                  ( 1, 9)  6             ( 1, 6)  6
                                                                                                  ( 2, 3)  6             ( 1, 7)  6
                                                                                                  ( 2, 4)  6             ( 1, 8)  6
                                                                                                  ( 2, 5)  6             ( 1, 9)  6
                                                                                                  ( 2, 6)  6             ( 2, 3)  6
                                                                                                  ( 2, 7)  6
                                                                                                  ( 2, 8)  6
                                                                                                  ( 2, 9)  6
                                                                                                  ( 3, 4)  6
                                                                                                  ( 3, 5)  6
                                                                                                  ( 3, 6)  6
                                                                                                  ( 3, 7)  6
                                                                                                  ( 3, 8)  6
                                                                                                  ( 3, 9)  6
                                                                                                  ( 4, 9)  6
                                                                                                  ( 5, 5)  6
                                                                                                  ( 5, 9)  6
                                                                                                  ( 6, 8)  5
                                                                                                  ( 7, 9)  6
                                                                                                  ( 8, 9)  6
                                                                                                  ( 9, 4)  6
FIN
```

FIGURE 4-6 SAMPLE PROBLEM OUTPUT (CONTINUED)

REFERENCES

4-1) Gref,L.G., and Rosengren,J.W., "An Assessment of Some Safeguards Evaluation Techniques," R and D Associates, RDA-TR-5000-002,February 1977

4-2) Glancy, J., Nicastro, J., Woolson, W., and El-Bassioni, A., "Analysis of Nuclear Fuel Facility Safeguards Against Threats Involving Insider Collusion," SAI-78-547-LJ, April 1978

4-3) Glancy, J., Nicastro, J., Woolson, W., and El-Bassioni, A., "Analysis of Nuclear Fuel Facility Safeguards Against Threats Involving Insider Collusion," SAI-78-547-LJ, Appendix B, "Application of the MAIT Method to the NRC Designated Facility," April 1978 (CONFIDENTIAL)

4-4) McDaniel, T., Glancy, J., and Horton, W., "Safeguards Against Insider Collusion," Vol. 1, "Guide on the Design of Work Rules for Safeguarding Against the Employee Collusion Threat at Nuclear Fuel Facilities," Science Applications, Inc., SAI-78-995-LJ, U. S. Nuclear Regulatory Commission report NUREG/CR-0532, December 1978

4-5) McDaniel, T. and Huszar, L., "Safeguards Against Insider Collusion," Vol. 2, "The MAIT (Matrix Analysis of the Insider Threat) Method for Analysis of Facility Safeguards Against Insider Collusion - User's Manual," Science Applications, Inc., SAI-78-960-LJ, U. S. Nuclear Regulatory Commission report NUREG/CR-0532, Vol2, June 1979

4-6) Davidson, R. and Rosengren, J., "An Assessment of Current Physical Security Models," R AND D Associates, RDA-TR-111500-001, October 1979

4-7) Monroe, R. W., "Analysis of the MAIT (Matrix Analysis of the Insider Threat) Computer Code for Use on the SNWS Program," NSWC TN 80-521, March 1981

4-8) McDaniel, T. and Huzar,L., "The MAIT (Matrix Analysis of the Insider Threat) User's Manual," Science Applications, Inc., SAI01581-210LJ, June 1981

DISTRIBUTION

	Copies
Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	12
Chief of Naval Operations (OP-403) Department of the Navy Washington, D. C. 20350	1
Commander Naval Sea Systems Command (SEA-64312C) Washington, D. C. 20360	2
Chief of Naval Material Attn: (C. Castells, MAT-04633) Washington, D. C. 20360	1
Department of the Army U.S. Army Meradcom Attn: (LaDonna Short, DRDME-ZPS) Ft. Belvoir, Virginia	1
Department of the Air Force Headquarters Electronics Systems Division Attn: (Physical Security Systems Directorate) Hanscom, Air Force Base, MA 01731	1
Library of Congress Attn: Gift and Exchange Division Washington, DC 20540	4

FILMED

9-8